Intro to Logic and Proofs

Propositions

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

Examples:

- It is raining today.
- Washington D.C. is the capital of the United States
- Houston is the capital of Texas.
- $1 + 1 = 2$.

Some sentences are not propositions (that is, no truth value can be assigned).

Examples:

- What time is it?
- Read this carefully.
- $x + 1 = 2$.
- $x + y = z$.

Truth Values and Propositional Variables

To each proposition a **truth value** is assigned: **T** for true and **F** for false.

We will often use **propositional variables** (most commonly: p, q, r, s, ...) to represent a proposition, especially when forming compound propositions.

Compound Propositions

Examples:

- It is not raining today. $(\neg p)$
- Today's temperature is 72 degrees, and the humidity is 50%. $(p \wedge q)$
- Washington D.C. is the capital of the United States, or Houston is the capital of Texas. $(p \vee q)$
- If it is raining today, then it is cloudy today. $(p \rightarrow q)$
- It is raining today if and only if it is cloudy. $(p \leftrightarrow q)$

Logical Connectives

1. negation ($\neg$)
2. conjunction ($\wedge$)
3. disjunction ($\vee$)
4. conditional ($\rightarrow$)
5. biconditional ($\leftrightarrow$)

1. Negation ($\neg p$)

The **negation** of a proposition p, denoted by $\neg p$, and read "not p", is the statement

$$\boxed{\neg p : \text{ "It is not the case that" } p}$$

The truth value of the negation of p is the opposite of the truth value of p.

2. Conjunction ($p \wedge q$)

The **conjunction** of two propositions p and q, denoted by $p \wedge q$, is the statement

$$\boxed{p \wedge q : \quad p \text{ “and” } q}$$

The conjunction $p \wedge q$ is true when both p and q are true, and is false otherwise.

3. Disjunction ($p \vee q$)

The **disjunction** of two propositions p and q, denoted by $p \vee q$, is the statement

$$\boxed{p \vee q : \quad p \text{ “or” } q}$$

The disjunction $p \vee q$ is false when both p and q are false, and is true otherwise.

3. Disjunction ($p \vee q$)

The logical connective $\vee$ is called **inclusive or**. This means if p and q are both true, then $p \vee q$ is true.

Note that the word "or" sometimes means **exclusive or**, denoted $\oplus$.

Example: "Soup or salad comes with an entree."

4. Conditional Statement ($p \to q$)

The **conditional statement** $p \to q$, is the proposition

$$\boxed{p \to q : \quad \text{“If”} \ p, \ \text{“then”} \ q}$$

The conditional statement $p \to q$ is false when p is true and q is false, and true otherwise.

p is called the hypothesis (or antecedent or premise) and q is called the conclusion (or consequence).

4. Conditional Statement ($p \to q$)

Note: There are many ways to express the conditional statement $p \to q$. Here are several common forms:

"if p, then q"
"if p, q"
"p is sufficient for q"
"a sufficient condition for q is p"
"q is necessary for p"
"a necessary condition for p is q"

"p implies q"
"p only if q"
"q if p"
"q when p"
"q whenever p"
"q follows from p"

5. Biconditional Statement ($\leftrightarrow$)

The **biconditional statement** $p \leftrightarrow q$, is the proposition

$$\boxed{p \leftrightarrow q : \quad p \text{ “if and only if” } q}$$

The conditional statement $p \leftrightarrow q$ is true when p and q have the same truth values, and is false otherwise.

5. Biconditional Statement ($\leftrightarrow$)

Common ways to express $p \leftrightarrow q$ in English:

"p if and only if q"

"p iff q"

"p is necessary and sufficient for q"

"p implies q, and conversely"

5. Biconditional Statement ($\leftrightarrow$)

Note: In informal language, a biconditional is sometimes expressed in the form of a conditional, where the converse is implied, but not stated. For example:

"If you finish your meal, then you can have dessert."

Truth tables ($\neg$, $\wedge$, $\vee$)

p	$\neg p$
T	
F	

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

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

Truth table ($p \to q$)

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

Example: If you score 100% on the final, then you get an A in the class.

p : You score 100% on the final.

q : You get an A in the class.

Truth table ($p \leftrightarrow q$)

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

Example: You get an A in the class if and only if your course average is 90% or above.

p : You get an A in the class.

q : Your course average is 90% or above.

Converse, Inverse, and Contrapositive

Given the conditional statement

$$\boxed{p \to q}$$

we sometimes refer to three related conditional statements

- **converse** $(q \to p)$
- **inverse** $(\neg p \to \neg q)$
- **contrapositive** $(\neg q \to \neg p)$

Example

p: It is raining today.

q: It is cloudy today.

- **original** $(p \rightarrow q)$:

  If it's raining, then it's cloudy.

- **converse** $(q \rightarrow p)$:

  If it's cloudy, then it's raining.

- **inverse** $(\neg p \rightarrow \neg q)$:

  If it's not raining, then it's not cloudy.

- **contrapositive** $(\neg q \rightarrow \neg p)$:

  If it's not cloudy, then it's not raining.

Truth table $(\neg q \to \neg p)$

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

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

Important Fact:

The contrapositive $(\neg q \to \neg p)$ always has the same truth-value as the original conditional $(p \to q)$.

Translating English Sentences

Let p, q, r be the propositions

p: You get an A on the final exam.
q: You do every exercise in the book.
r: You get an A in this class.

Translate:

(a) You get an A in this class, but you do not do every exercise in this book.

Translating English Sentences

Let p, q, r be the propositions

p: You get an A on the final exam.
q: You do every exercise in the book.
r: You get an A in this class.

Translate:

(b) To get an A in this class, it is necessary for you to get an A on the final.

Translating English Sentences

Let p, q, r be the propositions

p: You get an A on the final exam.
q: You do every exercise in the book.
r: You get an A in this class.

Translate:

(c) Getting an A on the final and doing every exercise in this book is sufficient for getting an A in this class.

Logical Equivalence

Compound propositions that have the same truth values in all possible cases are called **logically equivalent**.

The notation $p \equiv q$ means that propositions p and q are logically equivalent.

Equivalence of $p \to q$ and $\neg p \vee q$

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

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

Basic Equivalence Laws

De Morgan's Laws

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

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

Distributive Laws

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

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

Basic Equivalence Laws

Example: Use De Morgan's Law to express the negation of the given statement.

p : Jim has an iPhone and he has an iPad.

$\neg p$:

Basic Equivalence Laws

Example: Use the distributive law to express the given statement in an equivalent form.

p : Jim will have cookies, and he will have coffee or tea.

Logically equivalent statement:

Equivalence of $\neg(p \vee q)$ and $\neg p \wedge \neg q$

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

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

Equivalence of $\neg(p \wedge q)$ and $\neg p \vee \neg q$

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

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

Equivalence of $p \vee (q \wedge r)$ and $(p \vee q) \wedge (p \vee r)$

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

Equivalence of $p \wedge (q \vee r)$ and $(p \wedge q) \vee (p \wedge r)$

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

Logical Eqivalences

$p \wedge T \equiv p$ $p \vee F \equiv p$	Identity Laws
$p \vee T \equiv T$ $p \wedge F \equiv F$	Domination Laws
$p \vee p \equiv p$ $p \wedge p \equiv p$	Idempotent Laws
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Commutative Laws
$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Associative Laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption Laws

Logical Eqivalences

$\neg(\neg p) \equiv p$	Double Negation Law
$p \vee \neg p \equiv T$ $p \wedge \neg p \equiv F$	Negation Laws
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's Laws
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive Laws
$p \to q \equiv \neg p \vee q$	Material Implication

Constructing New Equivalences

From the preceding laws, one can deduce many other logical equivalences.

Example: Prove $\neg(p \vee (\neg p \wedge q)) \equiv \neg p \wedge \neg q$

Tautologies, Contradictions, and Contingencies

A compound proposition that is always true, no matter what the truth values of the propositional variables that occur in it, is called a **tautology**. (Example: $p \vee \neg p$)

A compound proposition that is always false is called a **contradiction**. (Example: $p \wedge \neg p$)

A compound proposition that is neither a tautology nor a contradiction is called a **contingency**. (Example: $p \rightarrow q$)

Predicates and Quantifiers

Quantifiers

Which of the following conditional statements can be assigned a truth value?

- If 1+1 = 2, then 2+2 =4.
- If the sky is blue, then the grass is green.
- If pigs can fly, then birds can fly.
- If $x > 7$, then $x > 5$.
- If x is an odd integer, then $2|x$.

Propositional Functions

A **propositional function** is a statement which depends on one or more variables, denoted $P(x)$, $Q(x, y)$, $R(x, y, z)$, etc., which takes the form of a proposition once a value is assigned for each variable.

Examples:

$$P(x): \quad x > 3$$

$$Q(x, y): \quad x = y + 3$$

$$R(x, y, z): \quad x + y = z$$

Propositional Functions

Example: Given the propositional functions

$$\begin{aligned} P(x): &\quad x > 3 \\ Q(x,y): &\quad x = y + 3 \\ R(x,y,z): &\quad x + y = z, \end{aligned}$$

express the following function values as propositions and determine their corresponding truth-values.

- $P(2)$:
- $Q(4,1)$:
- $R(2,-3,-1)$:

Quantifiers

In English, the words *all*, *some*, *many*, *none*, *few* are used to quantify a range of values for which a propositional function is true.

Examples:

- All even integers are divisible by 2.
- Some people have green eyes.
- Many people will attend the concert.
- None of the odd integers are divisible by 2.
- Few people will win the lottery.

Quantifiers

In mathematics we use the following quantifiers:

- **universal** quantifier ($\forall$)
- **existential** quantifier ($\exists$)

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

The **universal quantification** of $P(x)$, denoted $\forall x\, P(x)$, is the statement:

"For all x (in the **domain of discourse**), $P(x)$."

An element x for which $P(x)$ is false is called a **counterexample** of $\forall x\, P(x)$.

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

Alternate forms:

"For all x, $P(x)$."

"For every x, $P(x)$."

"For each x, $P(x)$."

"P(x), for all x."

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

The **existential quantification** of $P(x)$, denoted $\exists x\, P(x)$, is the statement:

"There exists an element x (in the **domain of discourse**) such that $P(x)$."

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

Alternate forms:

"There exists an x such that $P(x)$."

"There is at least one value x such that $P(x)$."

"There is an x such that $P(x)$."

"For some x, $P(x)$."

"$P(x)$, for some x."

Truth-values and Quantification

Statement	True when...	False when...
$\forall x\, P(x)$	$P(x)$ is true for every x.	There is an x for which $P(x)$ is false.
$\exists x\, P(x)$	There is an x for which $P(x)$ is true.	$P(x)$ is false for every x.

Truth-values and Quantification

Examples: Determine the truth-value of each statement. (In all cases assume the domain of discourse the set of real numbers.)

- $\forall x\,(x + 1 > x)$
- $\forall x\,(3x > 2x)$
- $\exists x\,(2x + 5 = 0)$
- $\exists x\,(x^2 = -1)$

Uniqueness Quantifier ($\exists! x\, P(x)$)

In mathematics, we often want to express that an equation or problem has a unique (one and only one) solution.

For this, we have a **uniqueness quantifier**, denoted $\exists!$. The statement $\exists!\, x\ P(x)$ reads

"There exists a unique element x such that $P(x)$."

Translating English Sentences

Express each statement in terms of quantifiers and the given propositional functions. Assume the domain of discourse is all people.

$P(x)$: x is a college student.

$Q(x)$: x pays tuition.

(a) Some people are college students.

(b) All college students pay tuition.

(c) Some college students pay tuition.

(d) All people who pay tuition are college students.

Bound Vs Free Variables

When a quantifier is used on a variable, we say that this variable is **bound**. A variable on which no quantifiers are used is called **free**.

Examples:

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

- $\exists z\,\forall y\,(x^2 + y^2 > z)$

Logical Equivalences and Quantifiers

Statements involving predicates and quantifiers are logically equivalent if and only if they have the same truth value no matter which predicates are substituted into these statements and which domain of discourse is used for the variables in these propositional functions.

Logical Equivalences and Quantifiers

Example:

$$\forall x(P(x) \wedge Q(x)) \equiv \forall x P(x) \wedge \forall x Q(x)$$

Proof: First assume the statement $\forall x(P(x) \wedge Q(x))$ is true. This means that if a is in the domain, then $P(a) \wedge Q(a)$ is true. Hence, $P(a)$ is true and $Q(a)$ is true. Because $P(a)$ is true and $Q(a)$ is true for every element in the domain, we can conclude that $\forall x\, P(x)$ and $\forall x\, Q(x)$ are both true. This means that $\forall x\, P(x) \wedge \forall x\, Q(x)$ is true.

Logical Equivalences and Quantifiers

Example:

$$\forall x(P(x) \wedge Q(x)) \equiv \forall x P(x) \wedge \forall x Q(x)$$

Proof: (*continued...*) Conversely, suppose the statement $\forall x\, P(x) \wedge \forall x\, Q(x)$ is true. It follows that $\forall x\, P(x)$ is true and $\forall x\, Q(x)$ is true. Hence, if a is in the domain, then $P(a)$ is true and $Q(a)$ is true. It follows that for all a, $P(a) \wedge Q(a)$ is true. It follows that $\forall x(P(x) \wedge Q(x))$ is true. Therefore we've shown:

$$\forall x(P(x) \wedge Q(x)) \equiv \forall x P(x) \wedge \forall x Q(x)$$

Negation of Quantifiers

We often want to consider the negation of a quantified statement.

Examples: Express the negation of each statement.

- S: All students take calculus.

  $\neg S$:

- S: Some students like homework.

  $\neg S$:

Negation of Quantifiers

Let's express the same statements in terms of quantifiers. First we define the propositional functions

$$P(x): \ x \text{ takes calculus.}$$
$$Q(x): \ x \text{ likes homework.}$$

- S: All students take calculus.

  S:

  $\neg S$:

  $\neg S$:

- S: Some students like homework.

  S:

  $\neg S$:

  $\neg S$:

De Morgan's Laws for Quantifiers

The previous examples illustrate the following two equivalences known as **De Morgan's laws for quantifiers**.

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

De Morgan's Laws for Quantifiers

Examples: Find the negation of each expression

- S: $\forall x\,(x^2 > x)$

  $\neg S$:

- S: $\exists x\,(x^2 = 2)$

  $\neg S$:

De Morgan's Laws for Quantifiers

Example: Show that

$$\neg(\forall x\,(P(x) \rightarrow Q(x))) \equiv \exists x\,(P(x) \wedge \neg Q(x))$$

Proof:

$\neg(\forall x\,(P(x) \rightarrow Q(x))) \equiv$

Nested Quantifiers

Nested quantifiers occur when one quantifier is within the scope of another.

Examples (Assume the domain of discourse is the set real numbers)

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

  For all real numbers x and y, the sum $x + y$ is equal to the sum $y + x$.

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

  For each real number x, there exists a real number y such that $x + y = 0$.

Order of Quantifiers

Note that changing the order of quantifiers may change the meaning and truth-value of an expression.

Example: Let $Q(x, y)$ denote "$x + y = 0$."

- $\forall x \, \exists y \, Q(x, y)$

  For each real number x, there exists a real number y such that $x + y = 0$.

- $\exists y \, \forall x \, Q(x, y)$

  There exists a real number y such that for all real numbers x, $x + y = 0$.

Truth-values and Nested Quantifiers

Statement	True when...	False when...
$\forall x \forall y\, P(x,y)$ $\forall y \forall x\, P(x,y)$	$P(x,y)$ is true for every pair x, y.	There is a pair x, y for which $P(x,y)$ is false.
$\forall x \exists y\, P(x,y)$	For every x there is a y for which $P(x,y)$ is true.	There is an x for which $P(x,y)$ is false for all y.
$\exists x \forall y\, P(x,y)$	There is an x for which $P(x,y)$ is true for all y.	For every x there is a y for which $P(x,y)$ is false.
$\exists x \exists y\, P(x,y)$ $\exists y \exists x\, P(x,y)$	There is a pair x, y for which $P(x,y)$ is true.	$P(x,y)$ is false for every pair x, y.

Translating Nested Quantifiers

Example: Translate the following

- $\forall x \, \forall y \, ((x > 0) \wedge (y < 0) \rightarrow (xy < 0))$

- $\forall x \, \forall y \, ((x + y < 0) \rightarrow (x < 0) \vee (y < 0))$

Translating Nested Quantifiers

Example: Translate the following

- If two numbers are unequal, then one of the numbers is less than the other.

- Every nonzero real number has a multiplicative inverse.

Negating Nested Quantifiers

To negate a statement with nested quantifiers we successively apply the rules for negating statements involving a single quantifier.

Example: Find the negation of

$$\forall x \, \exists y \, (xy = 1).$$

Negating Nested Quantifiers

Example: Find the negation of

$$\forall x \, \exists y \, (xy = 1).$$

To illustrate the process, we'll use the predicates

$$P(x, y): \quad xy = 1.$$
$$Q(x): \quad \exists y \, (xy = 1)$$

$\neg \forall x \, \exists y \, (xy = 1) \equiv$

Rules of Inference

Arguments and Validity

A formal **argument** in propositional logic is a sequence of propositions, starting with a **premise** or set of premises, and ending in a **conclusion**. We say that an argument is **valid** if and only if the conclusion is true when all premises are true.

Arguments and Validity

Example:

1. If I work, then I get paid.
2. If I get paid, then I pay the bills.

---

3. Therefore, if I work, then I pay the bills.

Argument Form

An **argument form** is a sequence of compound propositions involving propositional variables. An argument form is **valid** if no matter which particular propositions are substituted for the propositional variables in its premises, the conclusion is true if the premises are all true.

Example:

Argument	Argument Form
1. If I work, then I get paid. 2. If I get paid, then I pay the bills. 3. Therefore, if I work, then I pay the bills.	1. $p \rightarrow q$ 2. $q \rightarrow r$ 3. $\therefore p \rightarrow r$

Rules of Inference

Modus Ponens (Law of Detachment)

Example	Argument Form
1. If it snows today, then we will go skiing. 2. It is snowing today. 3. Therefore, we will go skiing.	$p \rightarrow q$ p $\therefore q$

Rules of Inference

Modus Tollens

Example	Argument Form
1. If it snows today, then we will go skiing. 2. We will not go skiing.	$p \rightarrow q$ $\neg q$
3. Therefore, it is not snowing today.	$\therefore \neg p$

Rules of Inference

Hypothetical Syllogism

Example	Argument Form
1. If I work, then I get paid. 2. If I get paid, then I pay the bills. 3. Therefore, if I work, then I pay the bills.	$p \rightarrow q$ $q \rightarrow r$ $\therefore p \rightarrow r$

Rules of Inference

Disjunctive syllogism

Example	Argument Form
1. It is sunny, or it is cloudy 2. It is not sunny. 3. Therefore, it is cloudy.	$p \vee q$ $\neg p$ $\therefore q$

Rules of Inference

Addition

Example	Argument Form
1. It is sunny. 2. Therefore, it is sunny, or it is cloudy.	p $\therefore p \vee q$

Rules of Inference

Simplification

Example	Argument Form
1. It is cloudy, and it is raining. 2. Therefore, it is cloudy.	$p \wedge q$ $\therefore p$

Rules of Inference

Conjunction

Example	Argument Form
1. It is cloudy. 2. It is raining.	p q
3. Therefore, it is cloudy, and it is raining.	$\therefore p \wedge q$

Rules of Inference

Resolution

Example	Argument Form
1. It's a weekday, or the kids are off of school. 2. It's not a weekday, or Jim is working. 3. Therefore, the kids are off of school, or Jim is working.	$p \vee q$ $\neg p \vee r$ $\therefore\ q \vee r$

Rules of Inference

Rule of Inference	Tautology	Name
p $\underline{p \to q}$ $\therefore q$	$(p \wedge (p \to q)) \to q$	Modus ponens
$\neg q$ $\underline{p \to q}$ $\therefore \neg p$	$(\neg q \wedge (p \to q)) \to \neg p$	Modus tollens
$p \to q$ $\underline{q \to r}$ $\therefore p \to r$	$((p \to q) \wedge (q \to r)) \to (p \to r)$	Hypothetical syllogism
$p \vee q$ $\underline{\neg p}$ $\therefore q$	$((p \vee q) \wedge \neg p) \to q$	Disjunctive syllogism

Rules of Inference

Rule of Inference	Tautology	Name
$\dfrac{p}{\therefore\ p \vee q}$	$p \rightarrow (p \vee q)$	Addition
$\dfrac{p \wedge q}{\therefore\ p}$	$(p \wedge q) \rightarrow p$	Simplification
$\dfrac{p \quad q}{\therefore\ p \wedge q}$	$(p \wedge q) \rightarrow (p \wedge q)$	Conjunction
$\dfrac{p \vee q \quad \neg p \vee r}{\therefore\ q \vee r}$	$((p \vee q) \wedge (\neg p \vee r) \rightarrow (q \vee r)$	Resolution
$\dfrac{p \rightarrow q}{\therefore\ \neg p \vee q}$	$(p \rightarrow q) \longrightarrow (\neg p \vee q)$	Material implication
$\dfrac{p \rightarrow q}{\therefore\ \neg q \rightarrow \neg p}$	$(p \rightarrow q) \longrightarrow (\neg q \rightarrow \neg p)$	Contraposition

Rules of Inference

Examples: In each case identify the rule of inference used.

- If it is cloudy, then it's raining. It's not raining. Therefore, it's not cloudy.

- If it rains today, then we will not have a barbecue today. If we do not have a barbecue today, then we will have a barbecue tomorrow. Therefore, if it rains today, then we will have a barbecue tomorrow.

Rules of Inference

Examples: In each case identify the rule of inference used.

- It is below freezing now. Therefore, it is either below freezing or raining now.

- It is below freezing and raining now. Therefore, it is below freezing now.

- Jasmine is skiing, or it is not snowing. It is snowing, or Bart is playing hockey. Jasmine is skiing, or Bart is playing hockey.

Rules of Inference

Examples:

- If you do every problem in this book, then you will learn discrete mathematics. You learned discrete mathematics. Therefore, you did every problem in this book.

- If you do every problem in this book, then you will learn discrete mathematics. You did not do every problem in this book. Therefore, you did not learn discrete mathematics.

Common Fallacies

Fallacy	Name
$p \to q$ q $\therefore p$	Affirming the conclusion
$p \to q$ $\neg p$ $\therefore \neg q$	Denying the hypothesis

Constructing Arguments

Example: For the given set of premises, what conclusion can be drawn?

1. It is not sunny today, and it is colder than yesterday.
2. We will go swimming only if it is sunny.
3. If we do not go swimming, then we will take a canoe trip.
4. If we take a canoe trip, then we will be home by sunset.

Conclusion:

Constructing Arguments

Premises

1. It is not sunny today, and it is colder than yesterday. $(\neg p \wedge q)$
2. We will go swimming only if it is sunny. $(r \rightarrow p)$
3. If we do not go swimming, then we will take a canoe trip. $(\neg r \rightarrow s)$
4. If we take a canoe trip, then we will be home by sunset. $(s \rightarrow t)$

Conclusion

We will be home by sunset. (t)

Argument

Statement	Reason
1. $\neg p \wedge q$	Premise
2. $\neg p$	Simplification (1)
3. $r \rightarrow p$	Premise
4. $\neg r$	Modus tollens (2 and 3)
5. $\neg r \rightarrow s$	Premise
6. s	Modus ponens (4 and 5)
7. $s \rightarrow t$	Premise
8. t	Modus ponens (6 and 7)

Constructing Arguments

Premises

1. If you send me an e-mail, then I will finish the project. $(p \rightarrow q)$
2. If you do not send me an e-mail, then I will go home. $(\neg p \rightarrow r)$
3. If I go home, then I will go to sleep early. $(r \rightarrow s)$

Conclusion

If I do not finish the project, then I will go to sleep early. $(\neg q \rightarrow s)$

Argument

Statement	Reason
1. $p \rightarrow q$	Premise
2. $\neg q \rightarrow \neg p$	Contrapositive (1)
3. $\neg p \rightarrow r$	Premise
4. $\neg q \rightarrow r$	Hypothetical syllogism (2 and 3)
5. $r \rightarrow s$	Premise
6. $\neg q \rightarrow s$	Hypothetical syllogism (4 and 5)

Rules of Inference and Quantifiers

Rule of Inference	Name
$\forall x\, P(x)$ $\therefore\ P(c)$ for an arbitrary c	Universal instantiation
$P(c)$ for an arbitrary c $\therefore\ \forall x\, P(x)$	Universal generalization
$\exists x\, P(x)$ $\therefore\ P(c)$ for some element c	Existential instantiation
$P(c)$ for some element c $\therefore\ \exists x\, P(x)$	Existential generalization

Rules of Inference and Quantifiers

Premises

D(x): "x is taking discrete math."
C(x): "x has taken calculus."

1. Everyone taking discrete math has taken calculus. $(\forall x(D(x) \rightarrow C(x)))$

2. Marla is taking discrete math class. $(D(Marla))$

Conclusion

Marla has taken calculus. $(C(Marla))$

Argument

Statement	Reason
1. $\forall x(D(x) \rightarrow C(x))$	Premise
2. D(Marla) $\rightarrow C$(Marla)	Universal instantiation (1)
3. D(Marla)	Premise
4. C(Marla)	Modus ponens (2 and 3)

Rules of Inference and Quantifiers

Premises

C(x): "x is in this class."
B(x): "x has read the book."
P(x): "x passed the class."

1. A student in this class has not read the book. $(\exists x(C(x) \wedge \neg B(x)))$

2. Everyone in this class passed the first exam. $(\forall x(C(x) \rightarrow P(x)))$

Conclusion

Someone who passed the first exam has not read the book.

$(\exists x(P(x) \wedge \neg B(x)))$

Argument

Statement	Reason
1. $\exists x(C(x) \wedge \neg B(x))$	Premise
2. $C(a) \wedge \neg B(a)$	Existential instantiation (1)
3. $C(a)$	Simplification (2)
4. $\forall x(C(x) \rightarrow P(x))$	Premise
5. $C(a) \rightarrow P(a)$	Universal instantiation (4)
6. $P(a)$	Modus ponens (3 and 5)
7. $\neg B(a)$	Simplification (2)
8. $P(a) \wedge \neg B(a)$	Conjunction (6 and 7)
9. $\exists x(P(x) \wedge \neg B(x))$	Existential generalization (8)

Introduction to Proofs

Mathematical Proofs

The rules of inference for **formal proofs** in propositional logic are the same as those used in **mathematical proofs**. However, in the latter case we allow for greater flexibility in the presentation of the argument. A mathematical proof often relies on many premises corresponding to the axioms of our mathematical system. For this reason, certain steps of the argument may be combined or assumed implicity for the sake of readability.

Types of Mathematical Statements

Axioms (or **postulates**) are basic mathematical statements that are assumed to be true.

The conclusion of a mathematical argument is called a **theorem**, **proposition**, **lemma**, or **corollary** depending on the relative importance of the statement. In particular, each represents a true mathematical statement supported by a proof.

A **conjecture** is mathematical statement which is believed to be true, but is unproven.

Integers and Parity

Definitions

We say that a number n is an **integer** if it belongs to the set

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

We say that an integer n is **odd** if there exists an integer k such that $n = 2k + 1$.

We say that an integer n is **even** if there exists an integer k such that $n = 2k$.

Theorem Forms

Many mathematical theorems have the form of a conditional or biconditional statement.

Examples:

1. If $x > y > 0$, then $x^2 > y^2$.

2. If $x, y \in \mathbb{Q}$, then $xy \in \mathbb{Q}$.

3. If n is an integer and $3n+2$ is odd, then n is odd.

4. An integer n is odd if and only if n^2 is odd.

Theorem Forms

Not all theorems have the form of a conditional statement. Identify the form of each of the following theorems.

Examples:

1. There are no perfect squares of the form $4k + 3$, where k is an integer.

2. For any real number x there exists a positive integer n, such that $x \leq n$.

3. $\sqrt{2}$ is an irrational number.

4. There are an infinite number of prime numbers.

Proof of a Conditional Statement ($p \to q$)

Methods

1. Direct Proof

2. Proof By Contraposition

3. Proof By Contradiction

Direct proof of $p \to q$

Strategy

Assume p is true, then use rules of inference to deduce q is true.

Direct Proof of $p \to q$

Theorem: If n is an odd integer, then $7n + 4$ is odd.

Proof:

Direct proof of $p \to q$

Theorem: If $x > y > 0$, then $x^2 > y^2$.

Proof:

Direct proof of $p \to q$

Theorem: If $x, y \in \mathbb{Q}$, then $xy \in \mathbb{Q}$.

Proof:

Direct proof of $p \to q$

Theorem: If n is an integer and $3n + 2$ is odd, then n is odd.

Proof:

Contraposition Proof of $p \to q$

Strategy

Assume $\neg q$ is true, then use rules of inference to deduce $\neg p$ is true.

What this shows...

This proves the contrapositive $\neg q \to \neg p$, which is logically equivalent to $p \to q$.

Contraposition Proof of $p \to q$

Theorem: If n is an integer and $3n + 2$ is odd, then n is odd.

Proof:

Contradiction Proof of $p \to q$

Strategy

Assume $p \wedge \neg q$ is true, then use rules of inference to deduce a false statement (a contradiction).

What this shows...

The fact that a valid argument produced a false statement means that the premise $p \wedge \neg q$ is false. Hence, $\neg(p \wedge \neg q)$, which is equivalent to $p \to q$, is true.

Contradiction Proof of $p \rightarrow q$

Theorem: If n is an integer and $3n + 2$ is odd, then n is odd.

Proof:

Proof of a Biconditional Statement ($p \leftrightarrow q$)

Strategy

Prove that both $p \rightarrow q$ and its converse, $q \rightarrow p$, are true. That is, (Step 1) assume p and deduce q, then (Step 2) assume q and deduce p.

Special Case (Reversible proof)

If q can be deduced from p using only inferences of the form "iff", then the argument is called **reversible** and only one step is required to complete the proof.

Proof of a Biconditional Statement ($p \leftrightarrow q$)

Theorem: An integer n is odd if and only if n^2 is odd.

Proof:

Proof of a Biconditional Statement ($p \leftrightarrow q$)

Theorem: $x^2 - 2x + 1 = 0$ if and only if $x = 1$.

Proof:

Contraposition Proof of $p \to q$

Theorem: If $x^2 - 2x - 3 > 0$, then $x < -1$ or $x > 3$.

Proof:

Proof by Cases

Theorem: $n^2 - 3n$ is even for all integers n.

Proof:

Proof by Contradiction (General Case)

Strategy

To prove a theorem of the form p by contradiction, we assume $\neg p$, then use rules of inference to deduce a false statement (a contradiction).

What this shows...

The fact that a valid argument produced a false statement means that the premise $\neg p$ is false. Hence, $\neg(\neg p)$, which is equivalent to p, is true.

Proof by Contradiction (General Case)

Theorem: There are no perfect squares of the form $4k + 3$, where k is an integer.

Proof:

Proof by Contradiction (General Case)

Theorem: For any real number x there exists a positive integer n, such that $x \leq n$.

Proof:

Proof by Contradiction (General Case)

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

Proof:

Proof by Contradiction (General Case)

Theorem: There are an infinite number of prime numbers.

Proof:

Theorems of Equivalence

Some theorems state the equivalence of a set of propositions $\{p_1, p_2, \ldots, p_n\}$.

Proof strategy

To prove $p_i \leftrightarrow p_j$ for all i and j, we use an n-step proof to establish a circular chain of implications

Step 1: $p_1 \rightarrow p_2$

Step 2: $p_2 \rightarrow p_3$

$\vdots$

Step n-1: $p_{n-1} \rightarrow p_n$

Step n: $p_n \rightarrow p_1$

Basic Concepts of Set Theory

Definition

A **set** is an unordered collection of objects, called elements or members of the set. A set is said to contain its elements. We write $a \in A$ to denote that a is an element of the set A. The notation $a \notin A$ denotes that a is not an element of the set A.

Defining a Set

The **roster method** is a way of defining a set by listing all of its members.

Examples

- The set of all vowels in the English alphabet is denoted by $\{a, e, i, o, u\}$.

- The set of odd positive integers is denoted by $\{1, 3, 5, \ldots\}$.

- The set of positive integers less than 100 is denoted by $\{1, 2, 3, \ldots, 99\}$.

Important Sets

Notation

$\mathbb{N} = \{1, 2, 3, \ldots\}$, the set of **natural numbers**, also denoted $\mathbb{Z}^+$.

$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, the set of **integers**

$\mathbb{Q}$, the set of **rational numbers**

$\mathbb{R}$, the set of **real numbers**

$\mathbb{R}^+$, the set of **positive real numbers**

$\mathbb{C}$, the set of **complex numbers**

Defining a Set

Another way to describe a set is using **set builder notation** which has the general form

$$S = \{x \in U \mid P(x)\},$$

where U is the **universal set** and $P(x)$ is a propositional function with domain U.

The set S consists of all elements in U such that $P(x)$ is true. This set is called the **truth set** of $P(x)$.

Defining a Set

Examples

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

$$= \{x \in \mathbb{N} \mid x \text{ is odd and } x < 10\}$$

$$= \{x \mid x \text{ is an odd positive integer less than } 10\}$$

$$\mathbb{Q} = \{x \in \mathbb{R} \mid Q(x)\}$$

where $Q(x)\colon\ \exists p\, \exists q\, (p \in \mathbb{N} \wedge q \in \mathbb{Z} \wedge x = \frac{p}{q})$

$$= \{x \in \mathbb{R} \mid x = \frac{p}{q}, \text{ where } p \in \mathbb{N} \text{ and } q \in \mathbb{Z}\}$$

Interval Notation

Recall the following notation for interval subsets of $\mathbb{R}$

$(a, b) = \{x \in \mathbb{R} \mid a < x < b\}$ **open interval**

$[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$ **closed interval**

$[a, b) = \{x \in \mathbb{R} \mid a \leq x < b\}$

$(a, b] = \{x \in \mathbb{R} \mid a < x \leq b\}$

$(-\infty, b] = \{x \in \mathbb{R} \mid x \leq b\}$

$(-\infty, b) = \{x \in \mathbb{R} \mid x < b\}$

$[a, \infty) = \{x \in \mathbb{R} \mid x \geq a\}$

$(a, \infty) = \{x \in \mathbb{R} \mid x > a\}$

Defining a Set

Example: Express the following set using set builder notation.

$S = \{\ldots, -12, -8, -4, 0, 4, 8, 12, \ldots\}$

The Empty Set

A set with no elements is called the **empty set**, or **null set**, and is denoted by $\emptyset$.

For example,

$$\{x \in \mathbb{R} \mid x^2 = -1\} = \emptyset.$$

Subsets

The set A is a **subset** of B if and only if every element of A is also an element of B. That is, A is a subset of B iff

$$\forall x\,(x \in A \rightarrow x \in B).$$

We use the notation $A \subseteq B$ to indicate that A is a subset of B.

Subsets

To show $A \subseteq B$

Assume $x \in A$, then show $x \in B$.

To show $A \nsubseteq B$

Show there exists an $x \in A$ such that $x \neq B$.

Subsets

Example: Consider the sets $A = \{2, -3\}$ and $B = \{x \in \mathbb{R} \mid x^3 + 3x^2 - 4x - 12 = 0\}$. Prove that $A \subseteq B$.

Proof:

Special Subsets

Theorem: For every set S,

(i) $\emptyset \subseteq S$

(ii) $S \subseteq S$

Proof of (i): By definition, $\emptyset \subseteq S$ iff

$$\forall x\,(x \in \emptyset \rightarrow x \in S).$$

Since the premise $x \in \emptyset$ is false for all x, the conditional statement is true for all x. This completes the proof of part (i).

Proof of (ii): By definition, $S \subseteq S$ iff

$$\forall x\,(x \in S \rightarrow x \in S).$$

Since the propositional form $p \rightarrow p$ is a tautology, the conditional statement is true for all x. This completes the proof of part (ii).

Proper Subsets

We say that A is a **proper subset** of B if and only if $A \subseteq B$ and $A \neq B$. That is, A is a proper subset of B iff

$$\forall x\,(x \in A \rightarrow x \in B) \wedge \exists x\,(x \in B \wedge x \notin A).$$

We use the notation $A \subsetneq B$ to indicate that A is a proper subset of B.

Equality of Sets

Two sets are **equal** if and only if they have the same elements. Therefore, if A and B are sets, then $A = B$ if and only if

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

That is, $A = B$ iff $A \subseteq B$ and $B \subseteq A$.

Equality of Sets

To show $A = B$

Step 1. Assume $x \in A$, then show $x \in B$.

Step 2. Assume $x \in B$, then show $x \in A$.

Equality of Sets

Example: Consider the sets $A = \{-1, 1\}$ and $B = \{x \in \mathbb{R} \mid x^2 = 1\}$. Prove that $A = B$.

Proof:

Equality of Sets

Remark

The sets $\{1, 2, 3\}$ and $\{2, 3, 1\}$ are equal, because they have the same elements. Note that the order in which the elements of a set are listed does not matter.

Equality of Sets

Theorem: If A and B are sets with no elements, then $A = B$.

Proof: By definition, $A = B$ iff

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

Since the sets A and B have no elements, the statements $x \in A$ and $x \in B$ are false for all x. Therefore, the biconditional statement $x \in A \leftrightarrow x \in B$ is true for all x. This completes the proof.

Power Sets

Let S be a set. The **power set** of S, denoted $\mathcal{P}(S)$, is the set of all subsets of S. That is,

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

Example: Let $S = \{a, b, c\}$. Then, $\mathcal{P}(S) =$

$$\{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

Note that the empty set $\emptyset$ and the set S itself are each members of $\mathcal{P}(S)$.

Power Sets

Examples: Find the power set of each of the following sets.

- $S = \{1, 2\}$

- $S = \emptyset$

- $S = \mathcal{P}(\emptyset)$

Power Sets

Theorem: If S is a set with n elements, then the power set $\mathcal{P}(S)$ is a set with 2^n elements.

Proof:

Let $S = \{s_1, s_2, s_3, \ldots, s_n\}$. To construct a subset T of S, we need to decide whether or not $s_i \in T$ for each $i = 1, 2, \ldots, n$. That is, for each $i = 1, 2, \ldots, n$, there are two possibilities, $s_i \in T$ or $s_i \notin T$, so there are

$$\underbrace{2 \cdot 2 \cdot 2 \cdot \cdots \cdot 2}_{n \text{ factors}} = 2^n$$

different ways of constructing a subset of S. Therefore $\mathcal{P}(S)$ has 2^n elements.

Set Operations

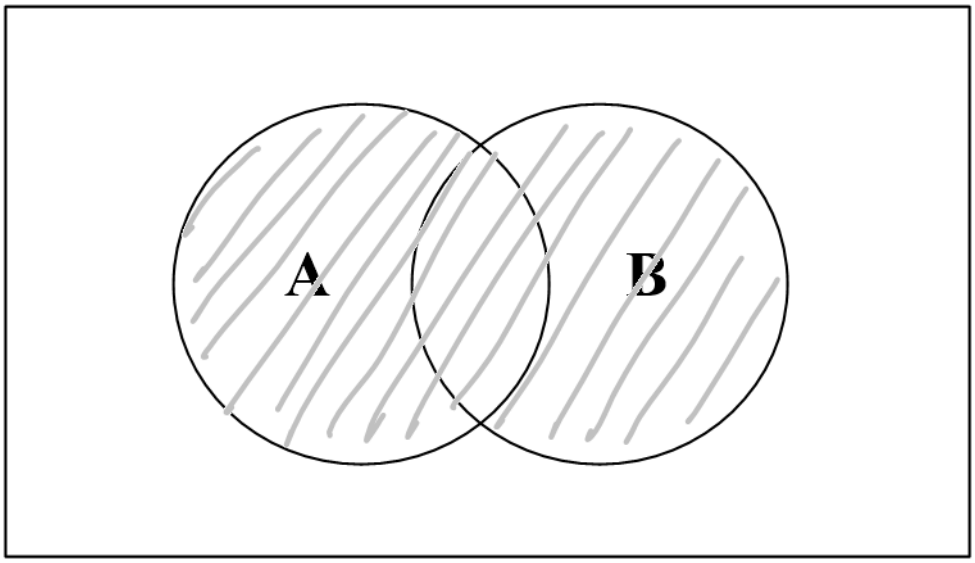
Union of Sets

Let A and B be sets. The **union** of the sets A and B, denoted by $A \cup B$, is the set that contains those elements that are either in A or in B, or in both. That is,

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

Union of Sets

Venn Diagram $(A \cup B)$



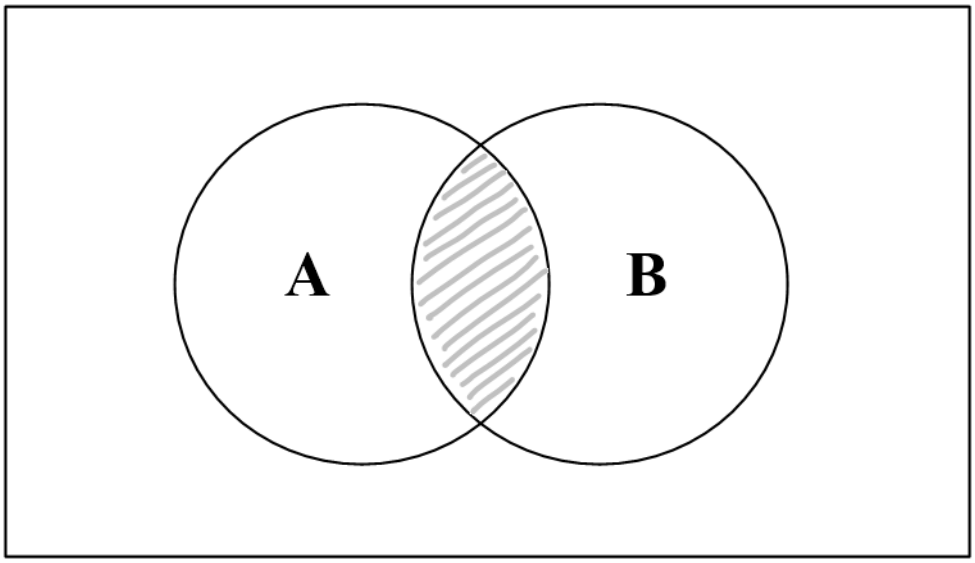
Intersection of Sets

Let A and B be sets. The **intersection** of the sets A and B, denoted by $A \cap B$, is the set containing those elements in both A and B. That is,

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

Intersection of Sets

Venn Diagram $(A \cap B)$



Union and Intersection

Example

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

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

$A \cap B = \{1, 3\}$

Disjoint Sets

Two sets are called **disjoint** if their intersection is the empty set.

Example

Let $A = \{1, 3, 5, 7, 9\}$ and $B = \{2, 4, 6, 8, 10\}$.

$A \cap B = \emptyset$, therefore A and B are disjoint.

Difference of Sets

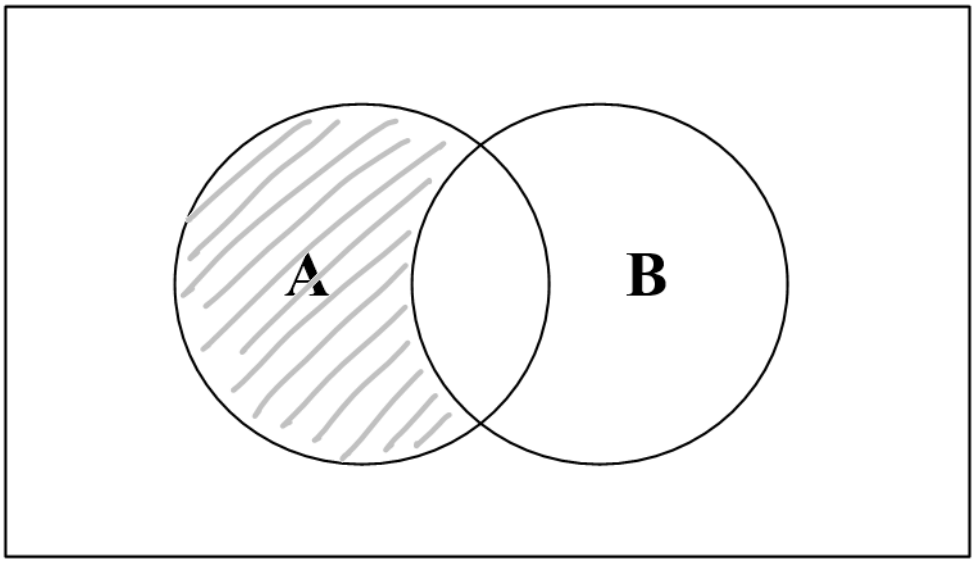
Let A and B be sets. The **difference** of A and B, denoted by $A - B$ (or $A \setminus B$), is the set containing those elements that are in A but not in B. That is,

$$A - B = \{x \mid x \in A \ \wedge \ x \notin B\}$$

The difference of A and B is also called the complement of B with respect to A.

Difference of Sets

Venn Diagram $(A - B)$



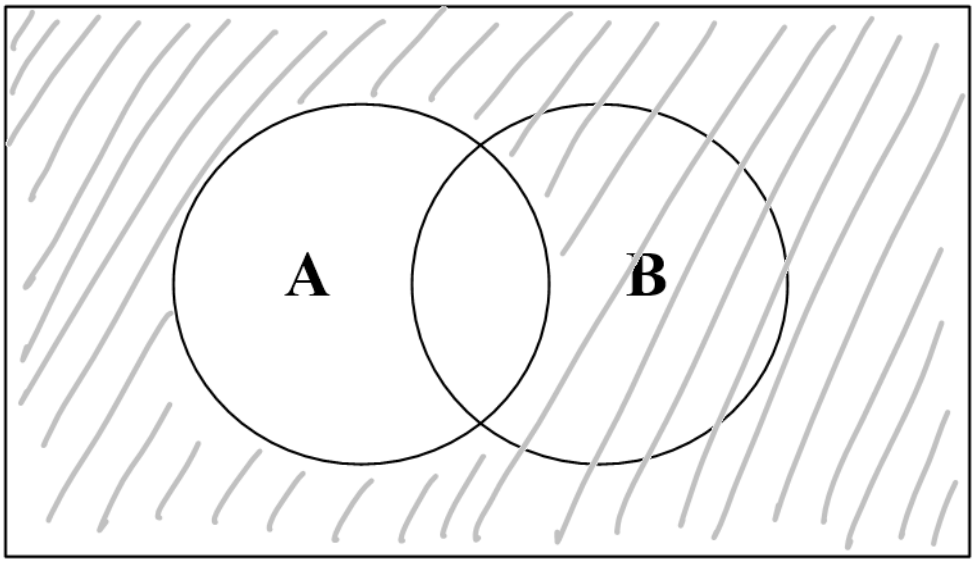
Complement of a Set

Let U be the universal set. The **complement** of the set A, denoted by A^{c}, is the complement of A with respect to U. That is

$$A^{\mathsf{c}} = U - A = \{x \mid x \in U \ \wedge \ x \notin A\}$$

Complement of a Set

Venn Diagram A^c



Complement of a Set

Example

Let U be the set of letters in the English alphabet, and let $V = \{a, e, i, o, u\}$. Then,

$$\begin{aligned} V^{\mathsf{c}} &= U - V \\ &= \{b, c, d, f, g, h, j, k, l, m, n, p, q, r, s, t, v, w, x, y, z\}. \end{aligned}$$

Set Operations

Example

Consider the universal set

$$U = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}.$$

If $A = \{1, 2, 4, 5, 7\}$ and $B = \{1, 3, 5, 9\}$, determine the following:

$A \cap B =$

$A \cup B =$

$A - B =$

$B - A =$

$A^{\mathsf{c}} =$

$B^{\mathsf{c}} =$

Set Identities

Identity	Name
$A \cap U = A$ $A \cup \emptyset = A$	Identity Laws
$A \cup U = U$ $A \cap \emptyset = \emptyset$	Domination Laws
$A \cup A = A$ $A \cap A = A$	Idempotent Laws
$(A^c)^c = A$	Double Complement Law
$A \cup A^c = U$ $A \cap A^c = \emptyset$	Complement Laws

Set Identities

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

Set Identities

Example: Prove the distributive law

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

Proof:

Set Identities

Example: Prove that $(A \cap B)^{\mathsf{c}} = A^{\mathsf{c}} \cup B^{\mathsf{c}}$

Proof:

Set Identities

Example: Use set identities to show that

$$(A \cup (B \cap C))^{\mathsf{c}} = (C^{\mathsf{c}} \cup B^{\mathsf{c}}) \cap A^{\mathsf{c}}$$

Sets and Proofs

Example: Prove that $A \cap B \subseteq A$.

Proof:

Sets and Proofs

Example: Prove that $A \subseteq B$ iff $A \cap B = A$.

Proof:

Sets and Proofs

Example: Prove that $A \cap (B - A) = \emptyset$.

Proof:

Ordered n-tuples

An **ordered n-tuple** $(a_1, a_2, \ldots, a_n)$ is an ordered collection that has a_1 as its first element, a_2 as its second element, ... , and a_n as its nth element.

Ordered 2-tuples are called **ordered pairs**.

Ordered n-tuples

We say that two ordered n-tuples are equal if and only if each corresponding pair of their elements is equal. In other words,

$$(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$$

if and only if

$$a_i = b_i, \quad \text{for } i = 1, 2, \ldots, n$$

Cartesian Product

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

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

Cartesian Product

Example:

If $A = \{1, 2\}$ and $B = \{a, b, c\}$, then

$A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$.

$B \times A = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}$.

Note that $A \times B \neq B \times A$, unless $A = B$.

Cartesian Product

The Cartesian product of the sets $A_1, A_2, \ldots, A_n$, denoted by $A_1 \times A_2 \times \cdots \times A_n$, is the set of ordered n-tuples $(a_1, a_2, \ldots, a_n)$, where a_i belongs to A_i for $i = 1, 2, \ldots, n$. In other words,

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i \text{ for } i = 1, 2, \ldots, n\}$$

Cartesian Product

Example:

If $A = \{1, 2\}$, $B = \{a, b, c\}$, and $C = \{\alpha, \beta\}$, then

$$A \times B \times C = \{(1, a, \alpha), (1, a, \beta), (1, b, \alpha), (1, b, \beta),$$
$$(1, c, \alpha), (1, c, \beta), (2, a, \alpha), (2, a, \beta),$$
$$(2, b, \alpha), (2, b, \beta), (2, c, \alpha), (2, c, \beta)\}$$

Cartesian Product

Notation

If A is a set, then A^n denotes the Cartesian product of n copies of A. That is,

$$A^n = \underbrace{A \times A \times \cdots \times A}_{n \text{ times}}$$

Extended Set Operations and Indexed Families of Sets

Set of Sets

A set of sets is often called a **family** or a **collection** of sets. We often use script letters, $\mathcal{A}, \mathcal{B}, \mathcal{C}, \ldots$, to denote families of sets. For example,

$$\mathcal{A} = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$$

$$\begin{aligned}\mathcal{B} &= \{\{1\}, \{1, 2\}, \{1, 2, 3\}, \ldots\} \\ &= \{\{1, 2, \ldots n\} \mid n \in \mathbb{N}\} \\ &= \{B_n \mid n \in \mathbb{N}\}\end{aligned}$$

$$\begin{aligned}\mathcal{C} &= \{(-\varepsilon, \varepsilon) \mid \varepsilon > 0\} \\ &= \{C_\varepsilon \mid \varepsilon \in \mathbb{R}^+\}\end{aligned}$$

Union of Sets

Let $\mathcal{A}$ be a family of sets. The **union** over $\mathcal{A}$, denoted $\bigcup_{A \in \mathcal{A}} A$, is the set of elements contained in at least one set in the family $\mathcal{A}$. That is,

$$\bigcup_{A \in \mathcal{A}} A = \{x \mid x \in A \text{ for some } A \in \mathcal{A}\}$$

Union of Sets

For a finite collection of sets $A_1, A_2, \ldots, A_n$, we use the notation

$$A_1 \cup A_2 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i$$

For a collection of sets $\{A_i\}_{i=1}^{\infty}$, we write

$$A_1 \cup A_2 \cup A_3 \cup \cdots = \bigcup_{i=1}^{\infty} A_i$$

Union of Sets

Examples

1. $\mathcal{A} = \{\emptyset, \{a\}, \{b\}, \{a, b\}\} = \{A_1, A_2, A_3, A_4\}$

$$\bigcup_{A \in \mathcal{A}} A = \bigcup_{i=1}^{4} A_i = A_1 \cup A_2 \cup A_3 \cup A_4 = \{a, b\}$$

2. $\mathcal{B} = \{\{1\}, \{1, 2\}, \{1, 2, 3\}, \ldots\} = \{B_1, B_2, B_3, \ldots\}$

$$\bigcup_{B \in \mathcal{B}} B = \bigcup_{i=1}^{\infty} B_i = B_1 \cup B_2 \cup B_3 \cup \ldots = \mathbb{N}$$

3. $\mathcal{C} = \{(-\varepsilon, \varepsilon) \mid \varepsilon > 0\} = \{C_\varepsilon \mid \varepsilon \in \mathbb{R}^+\}$

$$\bigcup_{C \in \mathcal{C}} C = \bigcup_{\varepsilon \in \mathbb{R}^+} C_\varepsilon = \mathbb{R}$$

Intersection of Sets

Let $\mathcal{A}$ be a family of sets. The **intersection** over $\mathcal{A}$, denoted $\bigcap_{A \in \mathcal{A}} A$, is the set of elements contained in every set in the family $\mathcal{A}$. That is,

$$\bigcap_{A \in \mathcal{A}} A = \{x \mid x \in A \text{ for every } A \in \mathcal{A}\}$$

Intersection of Sets

For a finite collection of sets $A_1, A_2, \ldots, A_n$, we use the notation

$$A_1 \cap A_2 \cap \cdots \cap A_n = \bigcap_{i=1}^{n} A_i$$

For a collection of sets $\{A_i\}_{i=1}^{\infty}$, we write

$$A_1 \cap A_2 \cap A_3 \cap \cdots = \bigcap_{i=1}^{\infty} A_i$$

Intersection of Sets

Examples

1. $\mathcal{A} = \{\varnothing, \{a\}, \{b\}, \{a, b\}\} = \{A_1, A_2, A_3, A_4\}$

$$\bigcap_{A \in \mathcal{A}} A = \bigcap_{i=1}^{4} A_i = A_1 \cap A_2 \cap A_3 \cap A_4 = \varnothing$$

2. $\mathcal{B} = \{\{1\}, \{1, 2\}, \{1, 2, 3\}, \ldots\} = \{B_1, B_2, B_3, \ldots\}$

$$\bigcap_{B \in \mathcal{B}} B = \bigcap_{i=1}^{\infty} B_i = B_1 \cap B_2 \cap B_3 \cap \ldots = \{1\}$$

3. $\mathcal{C} = \{(-\varepsilon, \varepsilon) \mid \varepsilon > 0\} = \{C_\varepsilon \mid \varepsilon \in \mathbb{R}^+\}$

$$\bigcap_{C \in \mathcal{C}} C = \bigcap_{\varepsilon \in \mathbb{R}^+} C_\varepsilon = \{0\}$$

Indexed Family of Sets

Let Δ be a nonempty set such that for each $\alpha \in \Delta$ there is a corresponding set A_α. The family

$$\{A_\alpha \mid \alpha \in \Delta\}$$

is an **indexed family of sets.** The set Δ is called the **indexing set** and each $\alpha \in \Delta$ is an **index**.

Indexed Family of Sets

Examples

1. $$\begin{aligned}\mathcal{A} &= \{\emptyset, \{a\}, \{b\}, \{a, b\}\} \\ &= \{A_1, A_2, A_3, A_4\} \\ &= \{A_n \mid n \in \{1, 2, 3, 4\}\}\end{aligned}$$

2. $$\begin{aligned}\mathcal{B} &= \{\{1\}, \{1, 2\}, \{1, 2, 3\}, \ldots\} \\ &= \{B_1, B_2, B_3, \ldots\} \\ &= \{B_n \mid n \in \mathbb{N}\}\end{aligned}$$

3. $$\begin{aligned}\mathcal{C} &= \{(-\varepsilon, \varepsilon) \mid \varepsilon > 0\} \\ &= \{C_\varepsilon \mid \varepsilon \in \mathbb{R}^+\}\end{aligned}$$

Indexed Family of Sets

Example Let $\Delta = \{0, 1, 2, 3, 4\}$, and let

$$A_\alpha = \{2\alpha + 4,\ 8,\ 12 - 2\alpha\}$$

for each $\alpha \in \Delta$. Determine the following

1. $A_0 = \{4, 8, 12\}$

2. $A_1 = \{6, 8, 10\}$

3. $A_2 = \{8\}$

4. $A_3 = \{6, 8, 10\}$

5. $A_4 = \{4, 8, 12\}$

6. $\mathcal{A} = \{A_\alpha \mid \alpha \in \Delta\} = \{\{4, 8, 12\}, \{6, 8, 10\}, \{8\}\}$

Indexed Family of Sets

Notation Let $\mathcal{A} = \{A_\alpha \mid \alpha \in \Delta\}$, then we express the union and intersection over $\mathcal{A}$ as follows

$$\bigcup_{A \in \mathcal{A}} A = \bigcup_{\alpha \in \Delta} A_\alpha$$

$$\bigcap_{A \in \mathcal{A}} A = \bigcap_{\alpha \in \Delta} A_\alpha$$

Indexed Family of Sets

Example Let $\Delta = \mathbb{Z}$, and let

$$A_\alpha = (\alpha, \alpha + 1)$$

for each $\alpha \in \Delta$. Determine the following:

1. $\bigcup_{\alpha \in \Delta} A_\alpha =$

2. $\bigcap_{\alpha \in \Delta} A_\alpha =$

Indexed Family of Sets

Example Let $\Delta = \mathbb{R}^+$, and let

$$A_\alpha = (-\infty, -\alpha) \cup (\alpha, \infty)$$

for each $\alpha \in \Delta$. Determine the following:

1. $\bigcup_{\alpha \in \Delta} A_\alpha =$

2. $\bigcap_{\alpha \in \Delta} A_\alpha =$

De Morgan's Law

Theorem Let $\mathcal{A} = \{A_\alpha \mid \alpha \in \Delta\}$ be an indexed collection of sets. Then,

1. $\left(\bigcup_{\alpha\in\Delta} A_\alpha\right)^c = \bigcap_{\alpha\in\Delta} A_\alpha^c$

2. $\left(\bigcap_{\alpha\in\Delta} A_\alpha\right)^c = \bigcup_{\alpha\in\Delta} A_\alpha^c$

Proof of (1):

$$x \in \left(\bigcup_{\alpha \in \Delta} A_\alpha \right)^{\mathsf{c}}$$

iff $x \notin \bigcup_{\alpha \in \Delta} A_\alpha$

iff it's not the case that $x \in \bigcup_{\alpha \in \Delta} A_\alpha$

iff it's not the case that $x \in A_\alpha$
for some $\alpha \in \Delta$

iff $x \notin A_\alpha$ for every $\alpha \in \Delta$

iff $x \in A_\alpha^{\mathsf{c}}$ for every $\alpha \in \Delta$

iff $x \in \bigcap_{\alpha \in \Delta} A_\alpha^{\mathsf{c}}$

Indexed Family of Sets

Example Let $\Delta = \mathbb{R}^+$, and let

$$A_\alpha = (-\infty, -\alpha) \cup (\alpha, \infty)$$

for each $\alpha \in \Delta$.

Verify Part 1 of De Morgan's Law:

1. $$\left(\bigcup_{\alpha \in \Delta} A_\alpha \right)^c = \left(\bigcup_{\alpha \in \Delta} (-\infty, -\alpha) \cup (\alpha, \infty) \right)^c$$

$$= ((-\infty, 0) \cup (0, \infty))^c$$

$$= \{0\}$$

2. $$\bigcap_{\alpha \in \Delta} A_\alpha^c = \bigcap_{\alpha \in \Delta} ((-\infty, -\alpha) \cup (\alpha, \infty))^c$$

$$= \bigcap_{\alpha \in \Delta} [-\alpha, \alpha]$$

$$= \{0\}$$

Pairwise Disjoint Sets

The sets in an indexed family

$$\mathcal{A} = \{A_\alpha \mid \alpha \in \Delta\}$$

are called **pairwise disjoint** if and only if

$$\forall\alpha\,\forall\beta\,[(A_\alpha = A_\beta) \vee (A_\alpha \cap A_\beta = \varnothing)]$$

Pairwise Disjoint Sets

Example Let $\Delta = \mathbb{Z}$, and let

$$A_\alpha = (\alpha, \alpha + 1)$$

for each $\alpha \in \Delta$.

The sets in $\mathcal{A} = \{A_\alpha \mid \alpha \in \Delta\}$ are pairwise disjoint since $A_\alpha \cap A_\beta = \emptyset$ for all $\alpha \neq \beta$.

Mathematical Induction

Peano Axioms

The set of natural numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$ has an implicit ordering, namely

$$1 < 2 < 3 < 4 < 5 < 6 < 7 < \cdots$$

We say that $n + 1$ is the **successor** of n. For example, 2 is the successor of 1, 3 is the successor of 2, and so on.

In terms of this notion of successor of an element, one can give a axiomatic description of the natural numbers from which the basic laws of arithmetic can be developed. These axioms are called **Peano Axioms.**

Peano Axioms

The structure of the natural numbers as an ordered set is characterized by the following five axioms:

(i) 1 is a natural number.

(ii) Every natural number has a unique successor, which is a natural number.

(iii) No two natural numbers have the same successor.

(iv) 1 is not the successor of any natural number.

(v) If a subset of the natural numbers contains the element 1 and contains the successors of all of its elements, then that subset contains all natural numbers.

Induction Axiom

Axiom (v) above is called the **induction axiom** and can be reformulated as follows:

If $S \subseteq \mathbb{Z}^+$ such that

(i) $1 \in S$,

(ii) $\forall k\,(k \in S \rightarrow k+1 \in S)$,

then $S = \mathbb{Z}^+$.

Induction as a Rule of Inference

In the context of mathematical proofs, the induction axiom serves as a rule of inference of the form

$$\frac{\begin{array}{l} P(1) \\ \forall k\,(P(k) \rightarrow P(k+1)) \end{array}}{\therefore\ \forall n\,(P(n))}$$

where P is any propositional function with domain $\mathbb{Z}^+$.

Mathematical Induction

Let $P(n)$ is a propositional function with domain $\mathbb{Z}^+$. To prove that $P(n)$ is true for all positive integers n, we complete two steps:

1. **(Base Case)** Verify that $P(1)$ is true.

2. **(Inductive Step)** Prove the conditional statement $P(k) \rightarrow P(k+1)$ is true for all positive integers k.

To complete the inductive step, we assume $P(k)$ is true (this assumption is called the **induction hypothesis**), then show $P(k+1)$ must also be true.

Mathematical Induction

Example: Show that if n is a positive integer, then

$$1 + 2 + 3 + \cdots n = \frac{n(n+1)}{2}$$

Mathematical Induction

Proof: Let $P(n)$ be the proposition

$$1 + 2 + 3 + \cdots n = \frac{n(n+1)}{2}.$$

We want to show $P(n)$ is true for all $n \geq 1$.

Base Step:

Mathematical Induction

Example: Conjecture a formula for the sum of the first n positive odd integers. Then prove your conjecture using mathematical induction.

$1 =$

$1 + 3 =$

$1 + 3 + 5 =$

$1 + 3 + 5 + 7 =$

$1 + 3 + 5 + 7 + 9 =$

Mathematical Induction

Conjecture: For all positive integers n, the following proposition $P(n)$ holds

$$1 + 3 + 5 + \cdots + 2n - 1 =$$

Proof:

Mathematical Induction

Example: Use mathematical induction to prove the inequality

$$n < 2^n$$

for all positive integers n.

Mathematical Induction

Proof: Let $P(n)$ be the proposition $n < 2^n$.

We want to show $P(n)$ is true for all $n \geq 1$.

Base Step:

Mathematical Induction

Example: Use mathematical induction to prove $n^3 - n$ is divisible by 3 for all $n \geq 1$.

Mathematical Induction

Proof: Let $P(n)$ be the proposition

$$3 \mid (n^3 - n).$$

We want to show $P(n)$ is true for all $n \geq 1$.

Base Step:

Generalized Induction

To prove that the propositional function $P(n)$ is true for all integers $\boxed{\boldsymbol{n \geq b}}$, we complete two steps:

1. **(Base Case)** Verify that $\boldsymbol{P(b)}$ is true.

2. **(Inductive Step)** Prove the conditional statement $P(k) \rightarrow P(k+1)$ is true for all positive integers $k \geq b$.

Generalized Induction

Example: Use generalized induction to show that for all nonnegative integers n

$$1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$$

Generalized Induction

Proof: Let $P(n)$ be the proposition

$$1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1.$$

We want to show $P(n)$ is true for all integers $n \geq 0$.

Generalized Induction

Example: Use generalized induction to prove that the sum of the first $n+1$ terms in a geometric progression with initial term a and common ratio $r \neq 1$ is given by

$$a + ar + ar^2 + \cdots + ar^n = \frac{ar^{n+1} - a}{r - 1}$$

Generalized Induction

Proof: Let $P(n)$ be the proposition

$$a + ar + ar^2 + \cdots + ar^n = \frac{ar^{n+1} - a}{r - 1}$$

We want to show $P(n)$ is true for all integers $n \geq 0$.

Generalized Induction

Example: Use generalized induction to prove the inequality

$$2^n < n!$$

for all integers $n \geq 4$.

Generalized Induction

Proof: Let $P(n)$ be the proposition

$$2^n < n!.$$

We want to prove that $P(n)$ is true for all integers $n \geq 4$.

Generalized Induction

Example: Use mathematical induction to prove that $7^{n+2} + 8^{2n+1}$ is divisible by 57 for all $n \geq 0$.

Generalized Induction

Proof: Let $P(n)$ be the proposition

$$\exists m\,(m \in \mathbb{Z} \ \wedge \ 7^{n+2} + 8^{2n+1} = 57m).$$

We want to show $P(n)$ is true for all $n \geq 0$.

Generalized Induction

Generalized De Morgan's Law

Let A_1, A_2, . . . , A_n be subsets of a universal set U, and let $P(n)$ be the proposition

$$\left(\bigcap_{j=1}^{n} A_j\right)^{\mathsf{c}} = \bigcup_{j=1}^{n} A_j^{\mathsf{c}}$$

Prove $P(n)$ is true for all $n \geq 2$.

Proof:

Base Step: The statement $P(2)$ asserts $(A_1 \cap A_2)^{\mathsf{c}} = (A_1)^{\mathsf{c}} \cup (A_2)^{\mathsf{c}}$, which is true by De Morgan's Law.

Inductive Step: Assume $P(k)$ is true for some fixed integer $k \geq 2$. That is, assume

$$\left(\bigcap_{j=1}^{k} A_j\right)^{\mathsf{c}} = \bigcup_{j=1}^{k} A_j^{\mathsf{c}}$$

for any collection of k sets A_1, A_2, . . . , A_k.

Then,

$$\begin{aligned}\left(\bigcap_{j=1}^{k+1} A_j\right)^{\mathsf{c}} &= \left[\left(\bigcap_{j=1}^{k} A_j\right) \cap A_{k+1}\right]^{\mathsf{c}} \\ &= \left(\bigcap_{j=1}^{k} A_j\right)^{\mathsf{c}} \cup A_{k+1}^{\mathsf{c}} \\ &= \left(\bigcup_{j=1}^{k} A_j^{\mathsf{c}}\right) \cup A_{k+1}^{\mathsf{c}} \\ &= \bigcup_{j=1}^{k+1} A_j^{\mathsf{c}}\end{aligned}$$

This completes the inductive step.

Therefore, $P(n)$ is true for all $n \geq 2$.

Complete Induction and the Well-Ordering Principle

Complete Induction as a Rule of Inference

In mathematical proofs, **complete induction** (PCI) is a rule of inference of the form

$$P(a) \wedge P(a+1) \wedge \cdots \wedge P(b)$$

$$\forall k \geq b \; ([\boldsymbol{P(a) \wedge P(a+1) \wedge \cdots \wedge P(k)}] \rightarrow P(k+1))$$

$$\therefore \forall n \geq a \; (P(n))$$

where a and b are positive integers with $a \leq b$, and P is any propositional function with domain $n \geq a$.

Complete Induction

To prove that a propositional function $P(n)$ is true for all positive integers $n \geq a$, we complete two steps:

1. **(Base Case)** Verify the truth of

$$P(a) \wedge P(a+1) \wedge \cdots \wedge P(b)$$

2. **(Inductive Step)** Prove the conditional statement

$$[\boldsymbol{P(a)} \wedge \boldsymbol{P(a+1)} \wedge \cdots \wedge \boldsymbol{P(k)}] \rightarrow P(k+1)$$

is true for all positive integers $k \geq b$.

To complete the inductive step, we assume $P(m)$ is true for all $m = a, a+1, a+2, \ldots, k$, then show $P(k+1)$ must also be true for all $k \geq b$.

Complete Induction

Special Case: $a = b = 1$

To prove that a propositional function $P(n)$ is true for all positive integers n, we complete two steps:

1. **(Base Case)** Verify that $P(1)$ is true.

2. **(Inductive Step)** Prove the conditional statement

   $$[P(1) \wedge P(2) \wedge P(3) \wedge \cdots \wedge P(k)] \rightarrow P(k+1)$$

   is true for all positive integers k.

Complete Induction

Special Case: $a = b = 1$

Example: Prove that every positive integer n has a binary expansion of the form

$$n = a_0 + a_1 2 + a_2 2^2 + \cdots + a_j 2^j,$$

where j is a nonnegative integer, $a_j = 1$, and $a_i \in \{0, 1\}$ for all i.

Complete Induction

Proof: Let $P(n)$ be the proposition:

$$n = a_0 + a_1 2 + a_2 2^2 + \cdots + a_j 2^j,$$

where j is a nonnegative integer, $a_j = 1$, and $a_i \in \{0, 1\}$ for all i.

We want to show $P(n)$ is true for all $n \geq 1$.

Base Step: $P(1)$ is true, since

$$1 = a_0 2^0$$

where $j = 0$ and $a_0 = 1$.

Inductive Step: Assume $P(m)$ is true for all positive integers $m \leq k$.

Then, consider the integer $k + 1$. We have two cases:

Case 1: (k+1 is even)

If $k+1$ is even, then $k+1 = 2m$ where $m \leq k$. Therefore, $P(m)$ is true and we have

$$\begin{aligned} k+1 &= 2m \\ &= 2(a_0 + a_1 2 + a_2 2^2 + \cdots + a_j 2^j) \\ &= 0 + a_0 2 + a_1 2^2 + a_2 2^3 + \cdots + a_j 2^{j+1} \\ &= \hat{a}_0 + \hat{a}_1 2 + \hat{a}_2 2^2 + \hat{a}_3 2^3 + \cdots + \hat{a}_{j+1} 2^{j+1} \end{aligned}$$

where $\hat{a}_{j+1} = a_j = 1$, $\hat{a}_0 = 0$, and $\hat{a}_i = a_{i-1} \in \{0, 1\}$ for all $1 \leq i \leq j$. Therefore, $P(k+1)$ is true in this case.

Case 2: (k+1 is odd)

If $k+1$ is odd, then $k = 2m$ where $m < k$.

Therefore, $P(m)$ is true and we have

$$\begin{aligned} k+1 &= 1+2m \\ &= 1+2(a_0+a_1 2+a_2 2^2+\cdots+a_j 2^j) \\ &= 1+a_0 2+a_1 2^2+a_2 2^3+\cdots+a_j 2^{j+1} \\ &= \hat{a}_0+\hat{a}_1 2+\hat{a}_2 2^2+\hat{a}_3 2^3+\cdots+\hat{a}_{j+1} 2^{j+1} \end{aligned}$$

where $\hat{a}_{j+1} = a_j = 1$, $\hat{a}_0 = 1$, and $\hat{a}_i = a_{i-1} \in \{0,1\}$ for all $1 \leq i \leq j$.

Therefore, $P(k+1)$ is true in either case. This completes the inductive step.

Therefore, it follows by complete induction that $P(n)$ is true for all $n \geq 1$.

Complete Induction

Example: Prove that every positive integer $n \geq 2$ can be expressed as a product of prime numbers.

Complete Induction

Proof: Let $P(n)$ be the proposition:

$$n = p_1\, p_2 \cdots p_j,$$

where $j \geq 1$ and p_i is prime for all j.

We want to show $P(n)$ is true for all $n \geq 2$. We will use complete induction corresponding to the case $a = b = 2$.

Base Step: $P(2)$ is true, since

$$2 = p_1$$

is a prime number.

Inductive Step: Assume $P(m)$ is true for all integers $m = a, a+1, \ldots, k$. That is, assume all integers $m = 2, 3, \ldots, k$ have a prime factorization.

Then, for $k \geq b = 2$, we have two cases.

Case 1: (k+1 is prime)

If $k+1 = p_1$ is prime, then $P(k+1)$ is true.

Case 2: (k+1 is composite)

If $k+1$ is composite, then there exist integers c and d with $1 < c \leq d < k+1$, such that

$$k+1 = c \cdot d$$

Then, $2 \leq c \leq k$ and $2 \leq d \leq k$, and it follows by the induction hypothesis that

$$c = p_1\, p_2 \cdots p_j$$

$$d = q_1\, q_2 \cdots q_\ell$$

where p_i and q_i are prime for all i. Thus,

$$k+1 = (p_1\, p_2 \cdots p_j) \cdot (q_1\, q_2 \cdots q_\ell)$$

and we conclude that $P(k+1)$ is true.

This completes the inductive step, and it follows by complete induction that $P(n)$ is true for all $n \geq 2$.

Well-Ordering Principle

Axiom: Every nonempty subset of $\mathbb{Z}^+$ has a least element.

That is, if $S \subseteq \mathbb{Z}^+$ and $S \neq \emptyset$, then S has a smallest element.

Well-Ordering Principle

Example: Use well-ordering property to prove the division algorithm:

If a is an integer and d is a positive integer, then there exist (unique) integers q and r with $0 \leq r < d$ such that $a = dq + r$.

Well-Ordering Principle

Proof: Consider the set

$$S = \{n \in \mathbb{Z}^+ \mid n = a - dq + 1 \text{ where } q \in \mathbb{Z}\}$$

This set is nonempty because $-dq$ can be made as large as desired (by taking $q < 0$ with $|q|$ sufficiently large). By the well-ordering principle, S has a least element $n_0 = (a - dq_0) + 1$ where $q_0 \in \mathbb{Z}$. We claim $n_0 \leq d$. If not, then

$$n_1 = (a - d(q_0 + 1)) + 1 = n_0 - d > 0,$$

which implies $n_1 \in S$ and $n_1 < n_0$. This contradicts the assumption that n_0 is the least element of S. Therefore, $1 \leq n_0 \leq d$.

This proves $a = dq_0 + r$ where $r = n_0 - 1$ is an integer such that $0 \leq r < d$.

The proof that q_0 and r are unique is left as an exercise.

Well-Ordering Principle

Theorem: The Well-Ordering Principle (WOP) and the Principle of Mathematical Induction (PMI) are equivalent.

WOP $\rightarrow$ PMI

Proof: Assume WOP holds. We want to prove PMI holds. Let $S \subseteq \mathbb{Z}^+$ such that

(i) $1 \in S$,

(ii) $k \in S \rightarrow k+1 \in S$ for all $k \in \mathbb{Z}^+$.

We want to prove $S = \mathbb{Z}^+$. Assume for the sake of contradiction that $S \neq \mathbb{Z}^+$. Then, $T = \mathbb{Z}^+ - S$ is a non-empty subset of $\mathbb{Z}^+$. Therefore, by the well-ordering principle, T has a least element m. That is, there exists $m \in T$ such that $m \leq n$ for all $n \in T$.

Since $1 \in S$, we know $m \geq 2$. Therefore $m-1$ is a positive integer. Clearly $m-1 \notin T$ (otherwise $m-1$ would be the least element

of T). This means $m-1 \in S$, and by assumption (ii)

$$(m-1) \in S \rightarrow (m-1)+1 \in S.$$

Therefore, $m \in S$ which contradicts the fact that $m \in T$.

We conclude that $S = \mathbb{Z}^+$. Therefore PMI holds.

Relations

Binary Relation

Let A and B be sets. A (binary) **relation** from A to B is a subset of $A \times B$.

Notation

Let $R \subseteq A \times B$ be a relation from A to B.

If $(a, b) \in R$, we write $a \, R \, b$.

Binary Relation

Example: Consider the sets $A = \{2, 3, 5, 7\}$ and $B = \{4, 6, 8, 9, 10\}$. Let R be the relation from A to B defined by

$$a \, R \, b \quad \text{iff} \quad b \text{ is divisible by } a.$$

Then R consists of the ordered pairs

$$\{(2, 4), (2, 6), (2, 8), (2, 10), (3, 6), (3, 9), (5, 10)\}.$$

Domain and Range

The **domain** of a relation R from A to B is the set

$$\mathrm{Dom}(R) = \{x \in A \mid \exists y\,(y \in B \text{ and } x\,R\,y)\}.$$

The **range** of the relation R from A to B is the set

$$\mathrm{Rng}(R) = \{y \in B \mid \exists x\,(x \in A \text{ and } x\,R\,y)\}.$$

Domain and Range

Example: Consider the sets $A = \{2, 3, 5, 7\}$ and $B = \{4, 6, 8, 9, 10\}$. Let R be the relation from A to B defined by

$$a \, R \, b \quad \text{iff} \quad b \text{ is divisible by } a.$$

Then R consists of the ordered pairs

$$\{(2, 4), (2, 6), (2, 8), (2, 10), (3, 6), (3, 9), (5, 10)\}.$$

Domain and Range

Example: Consider the sets $A = \{2, 3, 5, 7\}$ and $B = \{4, 6, 8, 9, 10\}$. Let R be the relation from A to B defined by

$$a \, R \, b \quad \text{iff} \quad b \text{ is divisible by } a.$$

Then R consists of the ordered pairs

$$\{(2, 4), (2, 6), (2, 8), (2, 10), (3, 6), (3, 9), (5, 10)\}.$$

$\text{Dom}(R) = \{2, 3, 5\}$

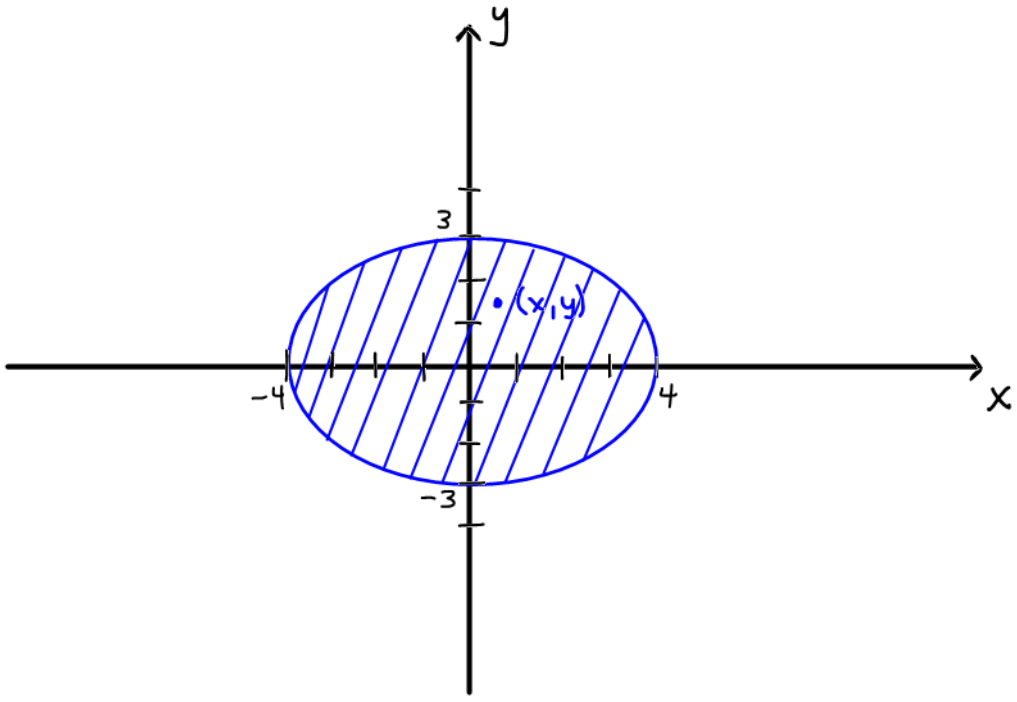
$\text{Rng}(R) = \{4, 6, 8, 9, 10\}$

Domain and Range

Example: Let $X = Y = \mathbb{R}$, and consider the relation R from X to Y defined by

$$x \, R \, y \quad \text{iff} \quad \frac{x^2}{16} + \frac{y^2}{9} \leq 1.$$

That is, $R = \left\{ (x, y) \in \mathbb{R} \times \mathbb{R} \;\middle|\; \frac{x^2}{16} + \frac{y^2}{9} \leq 1 \right\}$.



Domain and Range

Example: Let $X = Y = \mathbb{R}$, and consider the relation R from X to Y defined by

$$x \, R \, y \quad \text{iff} \quad \frac{x^2}{16} + \frac{y^2}{9} \leq 1.$$

That is, $R = \left\{ (x, y) \in \mathbb{R} \times \mathbb{R} \;\middle|\; \frac{x^2}{16} + \frac{y^2}{9} \leq 1 \right\}$.

$\text{Dom}(R) = [-4, 4]$

$\text{Rng}(R) = [-3, 3]$

Binary Relation on a Set

A (binary) **relation on a set** S is a relation from the set S to S.

Binary Relation on a Set

Examples: Let $S = \mathbb{R}$. The following are examples of binary relations on S.

$R_1 = \{(x, y) \mid x = y\}$,

$R_2 = \{(x, y) \mid x < y\}$,

$R_3 = \{(x, y) \mid x \leq y\}$,

$R_4 = \{(x, y) \mid x > y\}$,

$R_5 = \{(x, y) \mid x \geq y\}$,

$R_6 = \{(x, y) \mid x = y \text{ or } x = y\}$,

$R_7 = \{(x, y) \mid x = y + 1\}$,

$R_8 = \{(x, y) \mid x + y \leq 3\}$.

Identity Relation

The **identity relation** on S is the relation from S to itself given by

$$I_S = \{(x, x) \mid x \in S\}.$$

Example: Let $S = \{a, b, c\}$. The identity relation on S is the relation

$$I_S = \{(a, a), (b, b), (c, c)\}$$

Inverse Relation

If R is a relation from A to B, then the inverse of R, denoted R^{-1}, is the relation

$$R^{-1} = \{(y, x) \mid (x, y) \in R\}$$

Example: Consider the relation

$R = \{(2,4), (2,6), (2,8), (2,10), (3,6), (3,9), (5,10)\}$.

The inverse of R is the relation

$R^{-1} = \{(4,2), (6,2), (8,2), (10,2), (6,3), (9,3), (10,5)\}$.

Inverse Relation

Theorem: If R is a relation from A to B, then

(a) $\text{Rng}(R^{-1}) = \text{Dom}(R)$.

(b) $\text{Dom}(R^{-1}) = \text{Rng}(R)$.

Proof:

Inverse Relation

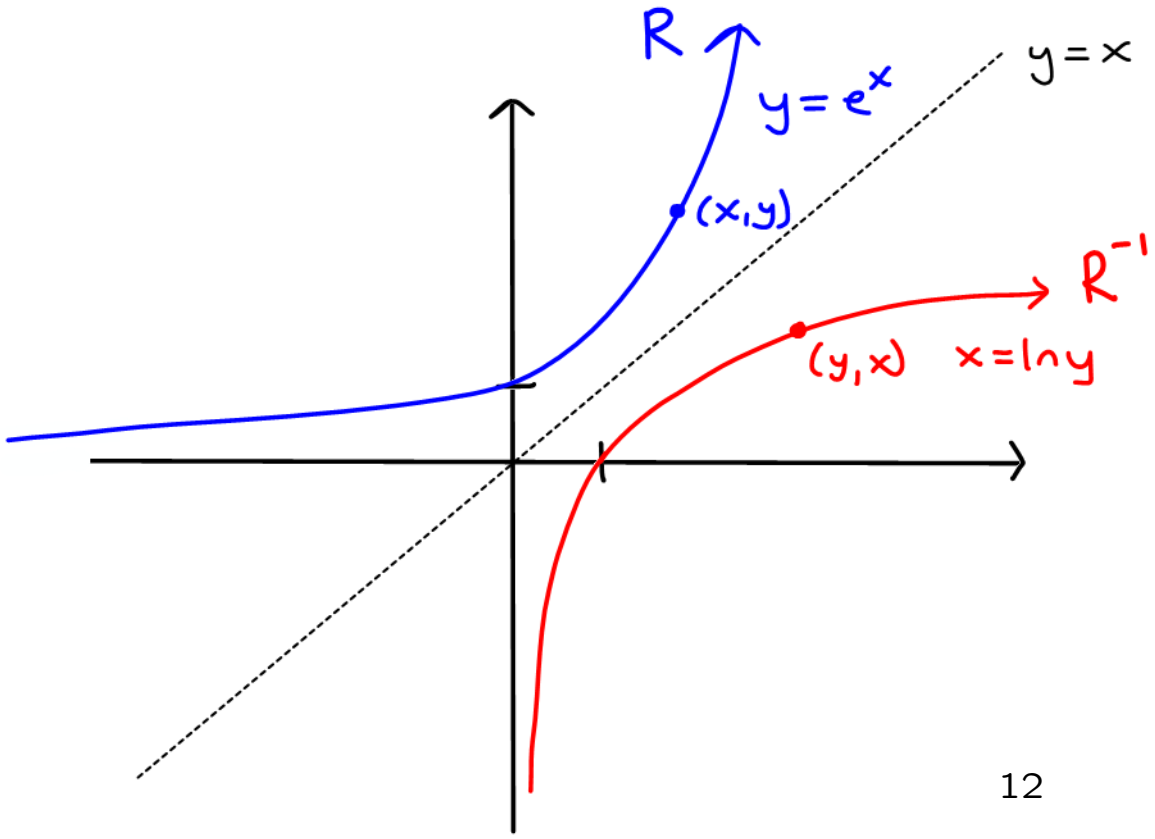
Example

Let R be the relation on $\mathbb{R}$ given by

$$x \, R \, y \quad \text{iff} \quad y = e^x.$$

The inverse of R is the relation given by

$$x \, R^{-1} \, y \quad \text{iff} \quad x = e^y \quad \text{iff} \quad y = \ln x.$$



Inverse Relation

Example

Let R be the relation on $\mathbb{R}$ given by

$$x \, R \, y \quad \text{iff} \quad y = e^x.$$

The inverse of R is the relation given by

$$x \, R^{-1} \, y \quad \text{iff} \quad x = e^y \quad \text{iff} \quad y = \ln x.$$

The previous theorem gives

$\text{Dom}(R^{-1}) = \text{Rng}(R) = (0, \infty)$.

$\text{Rng}(R^{-1}) = \text{Dom}(R) = (-\infty, \infty)$.

Composition of Relations

Let R be a relation from A to B, and let S be a relation from B to C.

The composition of R and S, denoted $S \circ R$, is a relation from A to C defined by

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

Composition of Relations

Example: Consider the sets

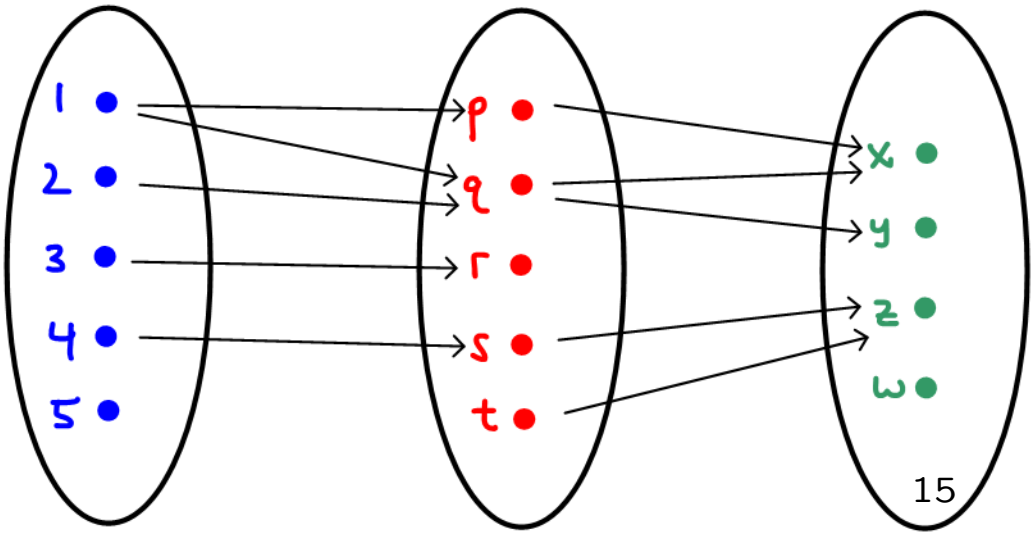
$$A = \{1, 2, 3, 4, 5\}$$
$$B = \{p, q, r, s, t\}$$
$$C = \{x, y, z, w\}$$

Let R be the relation from A to B given by

$$R = \{(1, p), (1, q), (2, q), (3, r), (4, s)\}.$$

Let S be the relation from B to C given by

$$S = \{(p, x), (q, x), (q, y), (s, z), (t, z)\}.$$



Composition of Relations

Example: Consider the sets

$$A = \{1, 2, 3, 4, 5\}$$
$$B = \{p, q, r, s, t\}$$
$$C = \{x, y, z, w\}$$

Let R be the relation from A to B given by

$$R = \{(1, p), (1, q), (2, q), (3, r), (4, s)\}.$$

Let S be the relation from B to C given by

$$S = \{(p, x), (q, x), (q, y), (s, z), (t, z)\}.$$

The composition $S \circ R$ is the relation from A to C given by

$$S \circ R = \{(1, x), (1, y), (2, x), (2, y), (4, z)\}.$$

Composition of Relations

Example: Consider the relations

$$R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = x + 1\}$$
$$S = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = x^2\}.$$

Determine the following:

$S \circ R =$

$R \circ S =$

Composition of Relations

Theorem: Suppose A, B, C, and D are sets. Let R be a relation from A to B, S be a relation from B to C, and T be a relation from C to D.

(a) $(R^{-1})^{-1} = R$.

(b) $T \circ (S \circ R) = (T \circ S) \circ R$.

(c) $I_B \circ R = R$ and $R \circ I_A = R$.

(d) $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$

Equivalence Relations

Reflexive Property

Let R be a relation on A. We say that R is **reflexive** if and only if $x\,R\,x$ for all $x \in A$.

Reflexive Property

Examples: Let $A = \{a, b, c\}$. In each case, decide if the given relation is reflexive.

- $R = \{(a, b),\ (b, a),\ (c, c)\}$.
- $R = \{(a, a),\ (a, c),\ (c, b),\ (a, b),\ (c, c)\}$.
- $R = \{(a, b),\ (b, b),\ (b, c)\}$.
- $R = \{(a, a),\ (a, b),\ (b, b),\ (b, a),\ (c, c)\}$.
- $R = \{(a, b),\ (a, c),\ (b, a),\ (b, c),\ (c, a),\ (c, b)\}$.
- $R = \{(a, a),\ (b, b),\ (c, c)\}$.

Symmetric Property

Let R be a relation on A. We say that R is **symmetric** if and only if

$$x\,R\,y \;\rightarrow\; y\,R\,x$$

for all $x, y \in A$.

Symmetric Property

Examples: Let $A = \{a, b, c\}$. In each case, decide if the given relation is symmetric.

- $R = \{(a, b),\ (b, a),\ (c, c)\}$.
- $R = \{(a, a),\ (a, c),\ (c, b),\ (a, b),\ (c, c)\}$.
- $R = \{(a, b),\ (b, b),\ (b, c)\}$.
- $R = \{(a, a),\ (a, b),\ (b, b),\ (b, a),\ (c, c)\}$.
- $R = \{(a, b),\ (a, c),\ (b, a),\ (b, c),\ (c, a),\ (c, b)\}$.
- $R = \{(a, a),\ (b, b),\ (c, c)\}$.

Transitive Property

Let R be a relation on A. We say that R is **transitive** if and only if

$$(x\,R\,y \ \wedge \ y\,R\,z) \ \rightarrow \ x\,R\,z$$

for all $x, y, z \in A$.

Transitive Property

Examples: Let $A = \{a, b, c\}$. In each case, decide if the given relation is transitive .

- $R = \{(a, b),\ (b, a),\ (c, c)\}$.
- $R = \{(a, a),\ (a, c),\ (c, b),\ (a, b),\ (c, c)\}$.
- $R = \{(a, b),\ (b, b),\ (b, c)\}$.
- $R = \{(a, a),\ (a, b),\ (b, b),\ (b, a),\ (c, c)\}$.
- $R = \{(a, b),\ (a, c),\ (b, a),\ (b, c),\ (c, a),\ (c, b)\}$.
- $R = \{(a, a),\ (b, b),\ (c, c)\}$.

Equivalence Relation

Let R be a relation on A. We say that R is an **equivalence relation** if and only if R is reflexive, symmetric, and transitive. That is, R is an equivalence relation iff

1. (Reflexivity)

   $x \, R \, x$, for all $x \in A$.

2. (Symmetry)

   if $x \, R \, y$, then $y \, R \, x$.

3. (Transitivity)

   if $x \, R \, y$ and $y \, R \, z$, then $x \, R \, z$.

Equivalence Relation

Example: Let $A = \{a, b, c\}$. List all equivalence relations on A.

- $R = \{(a, a),\ (b, b),\ (c, c)\}$
- $R = \{(a, a),\ (b, b),\ (c, c),\ (a, b),\ (b, a)\}$
- $R = \{(a, a),\ (b, b),\ (c, c),\ (b, c),\ (c, b)\}$
- $R = \{(a, a),\ (b, b),\ (c, c),\ (a, c),\ (c, a)\}$
- $R = \{(a, a),\ (b, b),\ (c, c),\ (a, b),\ (b, a)$
  $(a, c),\ (c, a),\ (b, c),\ (c, b)\}$

Equivalence Relation

Definition

Let n be a fixed positive integer. Given $x, y \in \mathbb{Z}$, we say that $\boldsymbol{x}$ **is congruent to** $\boldsymbol{y}$ **modulo** $\boldsymbol{n}$ if $x - y$ is divisible to n, and we write

$$x \equiv y \pmod{n}$$

The number n is called the modulus of the congruence.

Equivalence Relation

Example: Let R be the relation on $\mathbb{Z}$ defined by

$$x \, R \, y \quad \text{iff} \quad x \equiv y \pmod{n}$$

where n is a fixed positive integer. Prove that R is an equivalence relation.

Proof: Recall that $x \equiv y \pmod{n}$ if and only if $x - y = nk$ for some integer k.

(Reflexivity)

(i) $x \, R \, x$, since $x - x = 0 = n \cdot 0$.

(Symmetry)

(ii) Assume $x \, R \, y$. Then, $x - y = nk$ for some integer k. Therefore, $y - x = n(-k)$, where $-k$ is an integer. Therefore, $y \, R \, x$.

(Transitivity)

(iii) Assume $x \, R \, y$ and $y \, R \, z$. Then, $x - y = nk$ for some integer k, and $y - z = nj$ for some integer j. Then,

$$x - z = (x - y) + (y - z) = nk + nj$$

That is, $x - z = n(k + j)$ where $k + j$ is an integer. Therefore, $x \, R \, z$.

Equivalence Classes

Let R be an equivalence relation on a nonempty set A. Given $a \in A$, we define

$$[a] = \{x \in A \mid x \, R \, a\}.$$

That is, $[a]$ is the subset of elements in A which are related to a with respect to R.

The set $[a]$ is called the **equivalence class of a under R**. An element $x \in A$ is called a **representative** of $[a]$ if $x \in [a]$.

The collection of all equivalence classes with respect to R is called **A modulo R**, and is denoted

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

Equivalence Classes

Example

Find the equivalence class of each element of the set $A = \{a, b, c\}$ with respect to the equivalence relation

$$R = \{(a, a), (b, b), (c, c), (a, c), (c, a)\}.$$

$$[a] = \{a, c\}$$

$$[b] = \{b\}$$

$$[c] = \{a, c\}$$

Equivalence Classes

Example

Let R be the relation on $\mathbb{Z}$ defined by

$$x \, R \, y \quad \text{iff} \quad x \equiv y \pmod 4$$

Then,

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

where 0, 1, 2, and 3 are representatives of their respective equivalence classes.

Equivalence Classes

Theorem: Let R be an equivalence relation on a nonempty set A. For all $x, y \in A$,

(i) $[x] \subseteq A$ and $x \in [x]$.

Thus every equivalence class is a nonempty subset of A.

(ii) $[x] = [y]$ iff $x \, R \, y$.

Thus two elements of A have identical equivalence classes if and only if they are related.

(iii) $[x] \cap [y] = \emptyset$ iff $(x, y) \notin R$.

Thus two elements of A have disjoint equivalence classes if and only if they are not related.

Proof: Assume R is an equivalence relation on A. Then $a\,R\,a$ for all $a \in A$. Therefore $a \in [a]$ for all $a \in A$. This proves (i).

Next, assume $[x] = [y]$. Since $x \in [x]$, it follows that $x \in [y]$. Therefore, $x\,R\,y$.

Conversely, assume $x\,R\,y$. We want to show $[x] = [y]$. Assume $z \in [x]$. Then, $z\,R\,x$. Since $z\,R\,x$ and $x\,R\,y$, it follows by transitivity that $z\,R\,y$. Therefore, $z \in [y]$. This proves $[x] \subseteq [y]$.

On the other hand, assume $z \in [y]$. Then $z\,R\,y$. Also, by symmetry, $y\,R\,x$. Therefore, by transitivity, $z\,R\,x$. Therefore, $z \in [x]$. This shows $[y] \subseteq [x]$, which completes the proof of (ii).

Finally, assume $[x] \cap [y] = \emptyset$. Since $x \in [x]$, it follows that $x \notin [y]$. Therefore, $(x, y) \notin R$.

It remains to prove that if $(x, y) \notin R$, then $[x] \cap [y] = \emptyset$. We will use a proof by contraposition. Assume $[x] \cap [y] \neq \emptyset$. Then there exists an element $a \in A$ such that $a \in [x]$ and $a \in [y]$. Therefore, $a \, R \, x$ and $a \, R \, y$. By symmetry, $x \, R \, a$ and $a \, R \, y$. Therefore, by transitivity, $x \, R \, y$. This completes the proof of (iii).

Equivalence Classes

Theorem: Let R be the relation on $\mathbb{Z}$ defined by

$$x \, R \, y \quad \text{iff} \quad x \equiv y \pmod{n}$$

where n is a fixed positive integer. Then, the set of distinct equivalence classes with respect to R, denoted $\mathbb{Z}_n$, is given by

$$\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}.$$

Proof: Let $\mathbb{Z}_n$ denote the set of distinct equivalence classes with respect to R. First we will show $\mathbb{Z}_n \subseteq \{[0], [1], [2], \ldots, [n-1]\}$. Let $[a]$ be the equivalence class of some integer a. By the division algorithm, there exist integers q and r such that $a = qn + r$ where $0 \leq r < n$. Therefore, $a - r = qn$, which means $a \equiv r \pmod{n}$. It follows by the previous theorem that $[a] = [r]$. This proves $[a] \in \{[0], [1], [2], \ldots, [n-1]\}$.

It remains to show that the equivalence classes $[0], [1], [2], \ldots, [n-1]$ are all distinct. Assume for the sake of contradiction that there exist $j, k \in \mathbb{Z}$ such that $[j] = [k]$ and $0 \leq j < k < n$. It follows by the previous theorem that $j \equiv k \pmod{n}$. Therefore $k-j$ is divisible by n. However, $0 \leq j < k < n$ implies that $1 \leq k - j \leq n - 1$. This is a

contradiction. Therefore $[j] \neq [k]$ for all integers j and k such that $0 \leq j < k < n$. This completes the proof. $\square$

Partitions

Definition

Let A be a nonempty set. A **partition** of A is a collection $\mathcal{P}$ of nonempty subsets of A such that

(i) $\bigcup_{X \in \mathcal{P}} X = A$, and

(ii) If $X \in \mathcal{P}$ and $Y \in \mathcal{P}$, then $X = Y$ or $X \cap Y = \emptyset$.

In other words, a partition of A is a collection of *pairwise disjoint*, nonempty subsets of A whose union is A.

Partitions

Examples

- Let $A = \{1, 2, 3, 4, 5, 6\}$. Then,

  $$\mathcal{P} = \{\{1, 2\}, \{3, 4, 5\}, \{6\}\}$$

  is a partition of A.

- Let $A = \mathbb{Z}$. Then, $\mathcal{P} = \{Z_e, Z_o\}$ is a partition of A where

  $$Z_e = \{\ldots, -4, -2, 0, 2, 4, \ldots\},$$
  $$Z_o = \{\ldots, -3, -1, 1, 3, 5, \ldots\}$$

  are the set of even integers and odd integers, respectively.

Partitions

Examples

- Let $A = \mathbb{Z}^+$. Then,

  $\mathcal{P} = \{\{1\}, \{2, 3\}, \{4, 5, 6\}, \{7, 8, 9, 10\}, \ldots\}$

  is a partition of A.

- Let $A = \mathbb{R}$. Then,

  $$\mathcal{P} = \{G_n \mid n \in \mathbb{Z}\}$$

  is a partition of A where $G_n = [n, n + 1)$.

Equivalence Classes and Partitions

Theorem: If R is an equivalence relation on a nonempty set A, then A/R, the set of equivalence classes with respect to R is a partition of A.

Proof: Assume R is an equivalence relation on a nonempty set A. Previously, we proved that for all $a, b \in A$

$$(a, b) \in R \quad \text{iff} \quad [a] = [b],$$

and

$$(a, b) \notin R \quad \text{iff} \quad [a] \cap [b] = \emptyset.$$

Therefore, for all $a, b \in A$, we have

$$[a] = [b] \quad \text{or} \quad [a] \cap [b] = \emptyset.$$

This proves that the set of equivalence classes with respect to R are pairwise disjoint.

It remains to show that

$$\bigcup_{[a] \in A/R} [a] = A.$$

Clearly, $\bigcup_{[a] \in A/R} [a] \subseteq A$, since each equiva-

equivalence class [a] is a subset of A. Conversely, assume $x \in A$. Then,

$$x \in [x] \subseteq \bigcup_{[a] \in A/R} [a].$$

Therefore, $A \subseteq \bigcup_{[a] \in A/R} [a]$. This completes the proof.

□

Equivalence Classes and Partitions

Example

Let $A = \{a, b, c\}$. The distinct equivalence classes of the equivalence relation

$$R = \{(a, a), (b, b), (c, c), (a, c), (c, a)\}.$$

are $[a] = [c] = \{a, c\}$ and $[b] = \{b\}$. Hence,

$$A \,/\, R = \{\{a, c\}, \{b\}\}$$

is a partition of A.

Equivalence Classes and Partitions

Example

Let R be the relation on $\mathbb{Z}$ defined by

$$x \, R \, y \quad \text{iff} \quad x \equiv y \pmod 4$$

The distinct equivalence classes of R are

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

Hence,

$$\mathbb{Z} \, / \, R = \{[0], [1], [2], [3]\}$$

is a partition of $\mathbb{Z}$.

Equivalence Classes and Partitions

Theorem: Assume $\mathcal{P}$ is a partition of a nonempty set A. Let Q be the relation on A defined by

$x \, Q \, y$ iff $x \in S$ and $y \in S$ for some $S \in \mathcal{P}$.

Then,

(i) Q is an equivalence relation on A,

(ii) $A \,/\, Q = \mathcal{P}$.

Proof of (i): Assume $\mathcal{P}$ is a partition of a nonempty set A. Then, for all $x \in A$, there exists a set S in the partition $\mathcal{P}$ such that $x \in S$. Therefore, $x\,Q\,x$ for all $x \in A$. This proves Q is reflexive.

Next assume $x\,Q\,y$ where $x, y \in A$. Then there exists a set S in the partition $\mathcal{P}$ such that $x \in S$ and $y \in S$. Equivalently, we have $y \in S$ and $x \in S$. Hence, $y\,Q\,x$. This proves Q is symmetric.

Finally, assume that $x\,Q\,y$ and $y\,Q\,z$ where $x, y, z \in A$. Then there exist sets S and T in the partition $\mathcal{P}$ such that $x \in S$ and $y \in S$, and $y \in T$ and $z \in T$. Since $\mathcal{P}$ is a partition, we know $S = T$ or $S \cap T = \emptyset$. Since $y \in S \cap T$, it follows that $S = T$. Therefore, $x \in S$ and $z \in S$ which means $x\,Q\,z$. This proves Q is transitive.

Lemma: Assume $S \in \mathcal{P}$. Then, $x \in S$ if and only if $[x] = S$.

Proof: Assume $S \in \mathcal{P}$. We will divide the proof into two parts.

Part 1. ($x \in S$ implies $[x] = S$) Assume $x \in S$. We want to show that $[x] = S$. First, assume $y \in [x]$. Then, $y \, Q \, x$. Therefore there exists a set T in the partition $\mathcal{P}$ such that $y \in T$ and $x \in T$. Since $x \in S \cap T$, it follows that $S = T$. Hence $y \in S$. This shows $[x] \subseteq S$. On the other hand, assume $y \in S$. Then, $y \in S$ and $x \in S$. Hence $y \, Q \, x$. Therefore, $y \in [x]$. This proves $S \subseteq [x]$. Thus, $[x] = S$.

Part 2. ($[x] = S$ implies $x \in S$) Assume $[x] = S$. Then, $x \in S$, since $x \in [x]$. $\square$

Proof of (ii):

First, we want to show $A/Q \subseteq \mathcal{P}$. Assume $[x] \in A/Q$. There exists a set S in the partition $\mathcal{P}$ such that $x \in S$. Therefore, by the previous lemma, $[x] = S \in \mathcal{P}$.

Next, we want to show $\mathcal{P} \subseteq A/Q$. Assume $S \in \mathcal{P}$. Since S is nonempty, there exists an element $x \in S$. Therefore, by the previous lemma, $S = [x] \in A/Q$.

Therefore, $A/Q = \mathcal{P}$, and the proof is complete.

□

Ordering Relations

Comparability

Let R be a relation on a nonempty set A. Given $x, y \in A$, we say that x and y are **comparable** if $x\,R\,y$ or $y\,R\,x$.

Comparability

Example

Let R be the relation on $\mathbb{Z}^+$ defined by

$$x \, R \, y \quad \text{iff} \quad x \text{ is divisible by } y.$$

Then,

- $x = 2$ and $y = 6$ are comparable, since $(y, x) = (6, 2) \in R$.
- $x = 3$ and $y = 8$ are not comparable, since $(3, 8) \notin R$ and $(8, 3) \notin R$.

Comparability

Example

Let $X = \{1, 2, 3\}$, and let R be the relation on $\mathcal{P}(X)$ defined by

$$A \, R \, B \quad \text{iff} \quad A \subseteq B.$$

Then,

- the sets $A = \{1, 2, 3\}$ and $B = \{1, 3\}$ are comparable, since $B \subseteq A$.

- the sets $A = \{1, 2\}$ and $B = \{2, 3\}$ are not comparable, since $A \not\subseteq B$ and $B \not\subseteq A$.

Antisymmetric Property

Let R be a relation on A. We say that R is **antisymmetric** if and only if

$$x\,R\,y \;\wedge\; y\,R\,x \;\rightarrow\; x = y$$

for all $x, y \in A$.

Antisymmetric Property

Example

Let R be the relation on $\mathbb{Z}^+$ defined by

$$x \, R \, y \quad \text{iff} \quad x \text{ is divisible by } y.$$

Then, R antisymmetric.

Antisymmetric Property

Example

Let R be the relation on $\mathbb{Z}^+$ defined by

$$x\,R\,y \quad \text{iff} \quad x \text{ is divisible by } y.$$

Then, R antisymmetric.

Proof:

Assume x is divisible by y and y is divisible by x. Then, $x = jy$ and $y = kx$ where $j, k \in \mathbb{Z}^+$. Then, $x = j(kx)$. Therefore, $jk = 1$. Since j and k are positive integers, follows that $j = k = 1$. Hence, $x = y$.

Antisymmetric Property

Example

Let R be the relation on $\mathbb{R}$ defined by

$$x \, R \, y \quad \text{iff} \quad x \leq y.$$

Then, R antisymmetric, since $x \leq y$ and $y \leq x$ implies $x = y$.

Antisymmetric Property

Example

Let R be the relation on $\mathbb{R}$ defined by

$$x \, R \, y \quad \text{iff} \quad x < y.$$

Then, R antisymmetric, since the premise $x < y$ and $y < x$ is always false.

Antisymmetric Property

Example

Let X be a set, and let R be the relation on $\mathcal{P}(X)$ defined by

$$A \, R \, B \quad \text{iff} \quad A \subseteq B.$$

Then, R antisymmetric, since $A \subseteq B$ and $B \subseteq A$ implies $A = B$.

Partially Ordered Set

Let R be a relation on A. We say that R is a **partial order** if and only if R is reflexive, antisymmetric, and transitive.

A set A with partial order R is called a **partially ordered set**, or **poset**.

Partially Ordered Set

Example

Let R be the relation on $\mathbb{Z}$ defined by

$$x \, R \, y \quad \text{iff} \quad x \leq y \text{ and } x + y \text{ is even.}$$

Then, R is a partial order on $\mathbb{Z}$.

Note that $x \, R \, y$ if and only if $x \leq y$ and x and y have the same parity.

Proof:

(i) (R is reflexive.) For all $x \in \mathbb{Z}$, we have $x \leq x$ and $x + x = 2x$ is even. Therefore, $x \, R \, x$.

(ii) (R is antisymmetric.) Assume $x \, R \, y$ and $y \, R \, x$. Then, $x \leq y$ and $y \leq x$. Therefore, $x = y$.

(iii) (R is transitive.) Assume $x \, R \, y$ and $y \, R \, z$. Then, $x \leq y$ and $y \leq z$. Therefore, $x \leq z$. Also, there exist integers j and k such that $x + y = 2j$ and $y + z = 2k$. Therefore,

$$\begin{aligned} x + z &= (2j - y) + (2k - y) \\ &= 2j + 2k - 2y \\ &= 2(j + k - y). \end{aligned}$$

where $(j + k - y)$ is an integer. Hence, $x + z$ is even.

Digraphs

If A is a small finite set, we can use a **directed graph** or **digraph** to represent a relation R on A. Each element of A corresponds to a node in the graph called a **vertex**. Each ordered pair $(x, y) \in R$ is represented as a directed arrow from x to y called an **arc**. An arc from a vertex to itself is called a **loop**.

Digraphs

Example: In each case, draw the digraph for the given relation on $A = \{a, b, c\}$.

- $R = \{(a, b), (b, c), (c, a)\}$

- $R = \{(a, b), (b, a), (b, b), (c, b)\}$

- $R = \{(a,a),\ (b,b),\ (c,c),\ (a,b),\ (b,a)$
  $(a,c),\ (c,a),\ (b,c),\ (c,b)\}$

- $R = \{(a,a), (b,b), (c,c), (a,b), (b,a)\}$

- $R = \{(a,a), (b,b), (c,c)\}$

Partially Ordered Set

Theorem: Let R be a partial order on a nonempty set A. If

$$x\,R\,x_1,\quad x_1\,R\,x_2,\quad x_2\,R\,x_3,\quad \ldots,\quad x_n\,R\,x,$$

where $x, x_1, x_2, \ldots x_n \in A$, then

$$x = x_1 = x_2 = \cdots = x_n.$$

This means that the digraph of a partial order can never contain a **closed path** except for loops at individual vertices.

Proof: Let R be a partial order on a nonempty set A.

Base Step: Let $n = 1$. Assume $x\,R\,x_1$ and $x_1\,R\,x$. Then, by antisymmetry, $x = x_1$. This proves the proposition when $n = 1$.

Inductive Step: Assume that the proposition holds when $n = k$ is a fixed integer positive integer. We want to prove that the proposition also holds when $n = k + 1$.

Assume

$$x\,R\,x_1,\ \ x_1\,R\,x_2,\ \ x_2\,R\,x_3,\ \ \ldots,\ \ x_k\,R\,x_{k+1},\ \ x_{k+1}\,R\,x,$$

where $x, x_1, x_2, \ldots x_k, x_{k+1} \in A$. Since R is transitive, $x_k\,R\,x_{k+1}$ and $x_{k+1}\,R\,x$ implies $x_k\,R\,x$. Therefore we have

$$x\,R\,x_1,\ \ x_1\,R\,x_2,\ \ x_2\,R\,x_3,\ \ \ldots,\ \ x_k\,R\,x,$$

and it follows by the inductive hypothesis that

$$x = x_1 = x_2 = \cdots = x_k.$$

In particular, $x = x_k$. Therefore, $x \, R \, x_{k+1}$, since $x_k \, R \, x_{k+1}$. Then, by antisymmetry, $x \, R \, x_{k+1}$ and $x_{k+1} \, R \, x$ implies $x = x_{k+1}$. Therefore,

$$x = x_1 = x_2 = \cdots = x_k = x_{k+1},$$

which proves the proposition is true for $n = k + 1$.

Therefore, by induction, the proposition is true for all positive integers n.

□

Immediate Predecessor

Let R be a partial order on a nonempty set A, and let $a, b \in A$ with $a \neq b$. Then, a is an **immediate predecessor** of b iff $a \, R \, b$ and there does not exist $c \in A$ with $c \neq a$ such that $a \, R \, c$ and $c \, R \, b$.

Immediate Predecessor

Example

Let $A = \{1, 2, 3\}$, and consider the partial order

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

Then,

- 1 is an immediate predecessor of 2.
- 2 is an immediate predecessor of 3.
- 1 is *not* an immediate predecessor of 3.

Immediate Predecessor

Example

Let $A = \{1, 2, 3\}$, and consider the partial order $\subseteq$ on the power set $\mathcal{P}(A)$. Then,

- $\emptyset$ is an immediate predecessor of $\{1\}$, $\{2\}$, and $\{3\}$.
- $\{1\}$ is an immediate predecessor of $\{1, 3\}$ and $\{1, 2\}$.
- $\{1, 3\}$ is an immediate predecessor of $\{1, 2, 3\}$.
- $\{1\}$ is *not* an immediate predecessor of $\{1, 2, 3\}$, since $\{1\} \subseteq \{1, 2\} \subseteq \{1, 2, 3\}$.

Upper and Lower Bounds

Let R be a partial order on a nonempty set A, and let $B \subseteq A$. We say that an element $a \in A$ is an **upper bound** for B iff

$$b \, R \, a \quad \text{for all } b \in B.$$

We say that an element $a \in A$ is an **lower bound** for B iff

$$a \, R \, b \quad \text{for all } b \in B.$$

Upper and Lower Bounds

Example

Let $A = \mathcal{P}(X)$ where $X = \{1, 2, 3, 4\}$ and consider the partial order $\subseteq$ on A. Let $B = \{\{1, 4\}, \{2, 4\}\}$. Then,

- $\{1, 2, 3, 4\}$ is an upper bound for B.
- $\{1, 2, 4\}$ is an upper bound for B.
- $\emptyset$ is a lower bound for B.
- $\{4\}$ is a lower bound for B.

Supremum

Let R be a partial order on a nonempty set A, and let $B \subseteq A$. We say that an element $a \in A$ is a **least upper bound** or **supremum** for B iff

(i) a is an upper bound for B.

(ii) $a \, R \, x$ for every upper bound x of B.

The supremum of B is denoted **sup(B)**.

Infimum

Let R be a partial order on a nonempty set A, and let $B \subseteq A$. We say that an element $a \in A$ is a **greatest lower bound** or **infimum** for B iff

(i) a is a lower bound for B.

(ii) $x \, R \, a$ for every lower bound x of B.

The infimum of B is denoted **inf(B)**.

Infimum and Supremum

Example

Let $A = \mathcal{P}(X)$ where $X = \{1, 2, 3, 4\}$ and consider the partial order $\subseteq$ on A. Let $B = \{\{1, 4\}, \{2, 4\}\}$. Then,

- $\{1, 2, 3, 4\}$ is *not* a least upper bound for B.
- $\{1, 2, 4\}$ is a least upper bound for B.
- $\emptyset$ is *not* a greatest lower bound for B.
- $\{4\}$ is a greatest lower bound for B.

Infimum and Supremum

Theorem: Let R be a partial order on a nonempty set A, and let $B \subseteq A$. If $\sup(B)$ exists, it is unique. Also, if $\inf(B)$ exists, it is unique.

Proof:

Maximum and Minimum

Let R be a partial order on a nonempty set A, and let $B \subseteq A$. If $\sup(B)$ exists and $\sup(B) \in B$, then $\sup(B)$ is called the **largest element**, or **greatest element**, or **maximum element** of B.

If $\inf(B)$ exists and $\inf(B) \in B$, then $\inf(B)$ is called the **smallest element**, or **least element**, or **minimum element** of B.

Maximum and Minimum

Example

Let $A = \mathbb{R}$ and consider the partial order $\leq$ on A. Let $B = [0, 1)$. Then,

- Any real number $a \geq 1$ is an upper bound for B.
- Any real number $a \leq 0$ is a lower bound for B.
- $\inf(B) = 0$ and $\sup(B) = 1$.
- B does not have a maximum element, since $1 = \sup(B) \notin B$
- The minimum element of B is 0, since $0 = \inf(B) \in B$

Total Order

A partial order R on A is called a **total order**, or **linear order**, on A if any two elements x and y of A are comparable ($x\,R\,y$ or $y\,R\,x$).

Total Order

Examples

- The relation $\leq$ is a total order on each of the sets $\mathbb{Z}^+$, $\mathbb{Z}$, $\mathbb{R}$. (Alternatively, we say these sets are totally, or linearly, ordered by the relation $\leq$.)

- The relation $\subseteq$ on the set $\mathcal{P}(A)$ where $A = \{1, 2, 3\}$ (or any set A with two or more elements) is *not* a total order, since not all pairs of subsets are comparable. For example, $\{1, 2\} \not\subseteq \{2, 3\}$ and $\{2, 3\} \not\subseteq \{1, 2\}$.

Well Ordering

A total order R on a nonempty set A is called a **well ordering** on A iff every nonempty subset B of A contains a smallest element.

Well Ordering

Examples

- The relation $\leq$ is a well-ordering on the set $\mathbb{Z}^+$, since every collection of positive integers has a smallest element. (This is the Well Ordering Principle.)

- The relation $\leq$ is *not* a well ordering on the set $\mathbb{Z}$, since there are subsets of $\mathbb{Z}$ that are unbounded below (e.g., $A = \{\ldots, -3, -2, -1, 0\}$ has no smallest element.)

- The relation $\leq$ is *not* a well ordering on the set $\mathbb{R}$ (or even $[0, 1]$), since there are subsets of $\mathbb{R}$ that have no smallest

element (e.g., $A = (0, 1)$ has no smallest element.)

Well Ordering

Well-Ordering Theorem

Every set can be well ordered by some total order relation.

Proof: The proof requires the Axiom of Choice and will be revisited later.

Functions as Relations

Definition

Recall that if A and B are sets, then a **relation** from A to B is a subset of $A \times B$.

A **function** from A to B is a relation f from A to B with the following properties

(i) The domain of f is A.

(ii) If $(x, y) \in f$ and $(x, z) \in f$, then $y = z$.

In other words, for each $a \in A$, there is a unique element $b \in B$ such that $(a, b) \in f$.

Function Notation

If f is a function from A to B, we write

$$f : A \to B,$$

and we say that A is the **domain** of f and B is the **codomain** of f.

Functions

Example: Let $A = \{1, 2, 3\}$ and $B = \{4, 5, 6\}$. Determine which of the following relations are functions from A to B..

- $R = \{(1, 4), (2, 5), (3, 6), (2, 6)\}$
- $R = \{(1, 4), (2, 6), (3, 5)\}$
- $R = \{(1, 5), (2, 5), (3, 4)\}$
- $R = \{(1, 4), (3, 6)\}$

Functions

Example: Let $A = \{1, 2, 3\}$ and $B = \{4, 5, 6\}$. Determine which of the following relations are functions from A to B.

- $R = \{(1, 4), (2, 5), (3, 6), (2, 6)\}$

  R is not a function, since R is not "single-valued:"
  $(2, 5) \in R$ and $(2, 6) \in R$

- $R = \{(1, 4), (2, 6), (3, 5)\}$

  Function

- $R = \{(1, 5), (2, 5), (3, 4)\}$

  Function

- $R = \{(1, 4), (3, 6)\}$

  R is not a function from A to B, since $\text{Dom}(R) = \{1, 3\} \neq A$.

Functions

Example: Let F be the relation from $\mathbb{Z}$ to $\mathbb{Z}$ defined by

$$F = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid y = x^2\}.$$

Prove that F is a function from $\mathbb{Z}$ to $\mathbb{Z}$.

Proof:

Functions

Example: Let F be the relation from $\mathbb{Z}$ to $\mathbb{Z}$ defined by

$$F = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid y = x^2\}.$$

Prove that F is a function $\mathbb{Z}$ to $\mathbb{Z}$.

Proof: First we'll show that $\text{Dom}(F) = \mathbb{Z}$. Assume $x \in \mathbb{Z}$. Let $y = x^2$. Then, $y \in \mathbb{Z}$. Therefore, $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ and $y = x^2$, which means $(x, y) \in F$. Therefore, $x \in \text{Dom}(F)$. This proves $\text{Dom}(F) = \mathbb{Z}$.

Next, we'll show that F is "single-valued." Assume $(x, y) \in F$ and $(x, z) \in F$ where $x, y, z \in \mathbb{Z}$. Then $y = x^2$ and $z = x^2$. Therefore $y = z$. This completes the proof.

□

Functions

Example: Let F be the relation from $\mathbb{R}$ to $\mathbb{R}$ defined by

$$F = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x = y^3\}.$$

Prove that F is a function $\mathbb{R}$ to $\mathbb{R}$.

Proof:

Functions

Example: Let F be the relation from $\mathbb{R}$ to $\mathbb{R}$ defined by

$$F = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x = y^3\}.$$

Prove that F is a function $\mathbb{R}$ to $\mathbb{R}$.

Proof: First we'll show that $\text{Dom}(F) = \mathbb{R}$. Assume $x \in \mathbb{R}$. Let $y = \sqrt[3]{x}$. Then, $y \in \mathbb{R}$. Therefore, $(x, y) \in \mathbb{R} \times \mathbb{R}$ and $x = (\sqrt[3]{x})^3 = y^3$, which means $(x, y) \in F$. Therefore, $x \in \text{Dom}(F)$. This proves $\text{Dom}(F) = \mathbb{R}$.

Next, we'll show that F is "single-valued." Assume $(x, y) \in F$ and $(x, z) \in F$ where $x, y, z \in \mathbb{R}$. Then $x = y^3$ and $x = z^3$. Therefore $y^3 = z^3$. Therefore, $y = z$. This completes the proof.

□

Functions

Example: Let F be the relation from $\mathbb{R}$ to $\mathbb{R}$ defined by

$$F = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x = y^2\}.$$

Explain why F is *not* a function from $\mathbb{R}$ to $\mathbb{R}$.

Functions

Example: Let F be the relation from $\mathbb{R}$ to $\mathbb{R}$ defined by

$$F = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x = y^2\}.$$

Explain why F is *not* a function from $\mathbb{R}$ to $\mathbb{R}$.

Solution:

If $(x, y) \in F$, then $x = y^2 \geq 0$. Therefore the domain of F is $[0, \infty)$, not $\mathbb{R}$.

Also, F is not single-valued. For example, when $x = 4$, we have $y = \pm 2$. That is, $(4, 2) \in F$ and $(4, -2) \in F$. Hence, F is not a function.

Range of a Function

If $f : A \to B$ and the ordered pair (a, b) belongs to f, then we write

$$f(a) = b$$

and we say b the **image** of a under f.

The **range** of f, denoted Rng(f), is the set of all images of elements of A. That is,

$$\text{Rng}(f) = \{b \in B \mid (a, b) \in f \text{ for some } a \in A\}$$

Range of a Function

Example: Find the range of each function.

- $F : \mathbb{Z} \to \mathbb{Z}$ defined by $F(x) = x^2$.

  $\text{Rng}(F) = \{0, 1, 4, 9, 16, \ldots\}$

- $F : \mathbb{R} \to \mathbb{R}$ defined by $F(x) = \sin(x)$.

  $\text{Rng}(F) = [-1, 1]$

- $F : \{1, 2, 3\} \to \{4, 5, 6\}$ defined by

  $$F = \{(1, 5), (2, 5), (3, 4)\}.$$

  $\text{Rng}(F) = \{4, 5\}$

Composition of Functions

Theorem

Assume $f : A \to B$ and $g : B \to C$ are functions. Then the composite relation $g \circ f$, given by

$$\left\{(x, z) \in A \times C \;\middle|\; \exists y \left[(x, y) \in f \text{ and } (y, z) \in g\right]\right\}$$

is a function from A to C.

Proof: Assume $f : A \to B$ and $g : B \to C$ are functions. We want to show that the relation $g \circ f$ is a function from A to C.

First we want to show that the domain of $g \circ f$ is A. Since $g \circ f \subseteq A \times C$, we have $\text{Dom}(g \circ f) \subseteq A$. Conversely, assume $x \in A$. Since $f : A \to B$ is a function, there exists $y \in B$ such that $(x, y) \in f$. Then, since $g : B \to C$ is a function, there exists $z \in C$ such that $(y, z) \in g$. Therefore, $(x, z) \in g \circ f$, which shows $x \in \text{Dom}(g \circ f)$. This proves $\text{Dom}(g \circ f) = A$.

Next, we want to show that $g \circ f$ is single-valued. Assume $(x, z_1) \in g \circ f$ and $(x, z_2) \in g \circ f$. Then, there exist $y_1 \in B$ such that $(x, y_1) \in f$ and $(y_1, z_1) \in g$, and there exists $y_2 \in B$ such that $(x, y_2) \in f$ and $(y_2, z_2) \in g$.

In particular, $(x, y_1) \in f$ and $(x, y_2) \in f$, and since f is single-valued, it follows that $y_1 = y_2$. Then, $(y_1, z_1) \in g$ and $(y_1, z_2) = (y_2, z_2) \in g$, and since g is single-valued, it follows that $z_1 = z_2$. This proves $g \circ f$ is single-valued.

Therefore, $g \circ f$ is a function from A to B.

Composition of Functions

Theorem: Assume $f : A \to B$, $g : B \to C$, and $h : C \to D$ are functions. Then,

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

That is, composition of functions is associative.

Proof: By the previous theorem, we have

$$\begin{aligned}\mathrm{Dom}((h \circ g) \circ f) &= \mathrm{Dom}(f) = A,\\ \mathrm{Dom}(h \circ (g \circ f)) &= \mathrm{Dom}((g \circ f))\\ &= \mathrm{Dom}(f)\\ &= A.\end{aligned}$$

This shows that the domains of $(h \circ g) \circ f$ and $h \circ (g \circ f)$ are the same. Next, assume $x \in A$. Then,

$$\begin{aligned}((h \circ g) \circ f)(x) &= (h \circ g)(f(x))\\ &= h(g(f(x)))\\ &= h((g \circ f)(x))\\ &= (h \circ (g \circ f))(x).\end{aligned}$$

Therefore, $(h \circ g) \circ f = h \circ (g \circ f)$.

Composition of Functions

Example: Let $A = \{1, 2, 3, 4, 5\}$ and consider the functions $f, g : A \to A$ given by

$$f = \{(2, 4), (5, 1), (3, 2), (1, 2), (4, 3)\}$$
$$g = \{(4, 1), (5, 4), (1, 2), (2, 1), (3, 4)\}$$

Determine the following.

$(g \circ f)(1) =$

$(g \circ f)(2) =$

$(g \circ f)(3) =$

$(g \circ f)(4) =$

$(g \circ f)(5) =$

$g \circ f =$

$\text{Rng}(g \circ f) =$

Composition of Functions

Example: Let $A = \{1, 2, 3, 4, 5\}$ and consider the functions $f, g : A \to A$ given by

$$f = \{(2, 4), (5, 1), (3, 2), (1, 2), (4, 3)\}$$
$$g = \{(4, 1), (5, 4), (1, 2), (2, 1), (3, 4)\}$$

Determine the following.

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

$(g \circ f)(2) = g(f(2)) = g(4) = 1$

$(g \circ f)(3) = g(f(3)) = g(2) = 1$

$(g \circ f)(4) = g(f(4)) = g(3) = 4$

$(g \circ f)(5) = g(f(5)) = g(1) = 2$

$g \circ f = \{(1, 1), (2, 1), (3, 1), (4, 4), (5, 2)\}$

$\text{Rng}(g \circ f) = \{1, 2, 4\}$

One-To-One Function

Let $f : A \to B$. We say that f is **one-to-one**, or **injective**, if and only if

$$(x_1, y) \in f \ \wedge \ (x_2, y) \in f \quad \to \quad x_1 = x_2$$

for all $x_1, x_2 \in A$ and $y \in B$.

One-To-One Function

Equivalently, $f : A \to B$ is one-to-one if and only if for all $x_1, x_2 \in A$

$$f(x_1) = f(x_2) \quad \to \quad x_1 = x_2$$

If f is one-to-one, we say f is an **injection**.

Onto Function

Let $f : A \to B$. We say that f is **onto**, or **surjective**, if and only if for each $y \in B$ there exists $x \in A$ such that $f(x) = y$.

That is, f is onto if and only if the range of f is equal to the codomain of f.

If f is onto, we say that f is a **surjection**.

Examples

Let $A = \{1, 2, 3, 4\}$, $B = \{a, b, c\}$, $C = \{\alpha, \beta, \gamma\}$

Determine if the given functions are one-to-one, onto, both or neither.

1. $f : A \to B$ defined by $\begin{cases} f(1) = a \\ f(2) = b \\ f(3) = a \\ f(4) = b \end{cases}$

2. $f : B \to C$ defined by $\begin{cases} f(a) = \beta \\ f(b) = \gamma \\ f(c) = \alpha \end{cases}$

3. $f : B \to A$ defined by $\begin{cases} f(a) = 3 \\ f(b) = 1 \\ f(c) = 4 \end{cases}$

4. $f : A \to C$ defined by $\begin{cases} f(1) = \alpha \\ f(2) = \beta \\ f(3) = \beta \\ f(4) = \gamma \end{cases}$

Proof Strategy

To show f is injective

Show that if $f(x) = f(y)$, then $x = y$.

To show f is not injective

Show that there exist x and y such that $f(x) = f(y)$ and $x \neq y$.

To show f is surjective

Show that for each element y in the codomain there exists an element x in the domain such that $f(x) = y$.

To show f is not surjective

Show there exists an element y in the codomain such that $y \neq f(x)$ for any x in the domain.

Example

Prove or disprove:

The function $f : \mathbb{Z} \to \mathbb{Z}$ defined by

$$f(n) = 2n - 3$$

is injective.

Example

Prove or disprove:

The function $f : \mathbb{Z} \to \mathbb{Z}$ defined by

$$f(n) = 2n - 3$$

is injective.

f is injective.

Proof: For all $n, m \in \mathbb{Z}$ we have

$$\begin{array}{lll} f(n) = f(m) & \text{iff} & 2n - 3 = 2m - 3 \\ & \text{iff} & 2n = 2m \\ & \text{iff} & 2n - 2m = 0 \\ & \text{iff} & 2(n - m) = 0 \\ & \text{iff} & (n - m) = 0 \\ & \text{iff} & n = m. \end{array}$$

In particular, $f(n) = f(m)$ implies $n = m$ for all $n, m \in \mathbb{Z}$, which proves that f is injective.

□

Note that we did not multiply both sides of the equation $2n = 2m$ by $1/2$, since the codomain of f is $\mathbb{Z}$ and $1/2$ is not an integer.

Example

Prove or disprove:

The function $f : \mathbb{Z} \to \mathbb{Z}$ defined by

$$f(n) = 2n - 3$$

is surjective.

Example

Prove or disprove:

The function $f : \mathbb{Z} \to \mathbb{Z}$ defined by

$$f(n) = 2n - 3$$

is surjective.

f is not surjective.

The range of f contains only odd integers, therefore $\text{Rng}(f) \neq \mathbb{Z}$. For example,

$$0 \notin \text{Rng}(f)$$

since the equation $f(n) = 2n - 3 = 0$ has no solution in the domain $\mathbb{Z}$.

Example

Prove or disprove:

The function $f : \mathbb{Z} \to \mathbb{Z}$ defined by

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

is injective.

Example

Prove or disprove:

The function $f : \mathbb{Z} \to \mathbb{Z}$ defined by

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

is injective.

f is not injective.

Let $n = 1$ and $m = 4$. Then,

$$f(n) = f(1) = 1 + 1 = 2,$$

and

$$f(m) = f(4) = 4/2 = 2.$$

Therefore $f(m) = f(n)$, but $m \neq n$. This proves f is *not* injective.

Example

Prove or disprove:

The function $f : \mathbb{Z} \to \mathbb{Z}$ defined by

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

is surjective.

Example

Prove or disprove:

The function $f : \mathbb{Z} \to \mathbb{Z}$ defined by

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

is surjective.

f is surjective.

Proof: We want to show that for all $m \in \mathbb{Z}$ (codomain), there exists $n \in \mathbb{Z}$ (domain) such that $f(n) = m$.

Assume $m \in \mathbb{Z}$. Let $n = 2m$. Then, n is an even integer. Therefore,

$$f(n) = n/2 = 2m/2 = m.$$

This proves there exists an integer n, namely $n = 2m$, such that $f(n) = m$. Therefore, f is surjective.

Note that if n is odd, then $f(n) = n + 1$ is even. So if m is an even number in the codomain, then there are both even and odd values of n that map to m. Either $n = 2m$ (even) as above, or $n = m - 1$ (odd), which gives

$$f(n) = n + 1 = (m - 1) + 1 = m.$$

Since the former choice works even in the case when m is odd, there was no need to consider the latter choice for n.

Bijection

A function $f : A \to B$ is said to be a **bijection**, or **one-to-one correspondence** if f is both one-to-one and onto.

Examples

- $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = n + 1$
- $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 2x$
- $f : \mathbb{Z}^+ \to \mathbb{Z}^+$ defined by $f(n) = \begin{cases} n+1 & \text{if n is odd} \\ n-1 & \text{if n is even} \end{cases}$

Bijection

Example: Prove that $f : \mathbb{R}^+ \to (0, 1)$, defined by

$$f(x) = \frac{1}{1+x}$$

is a bijection.

Proof: We want to show that f is one-to-one (injective) and onto (surjective).

Step 1. (f is one-to-one.) For all $x_1, x_2 \in \mathbb{R}^+$ we have

$$\begin{aligned} f(x_1) = f(x_2) \qquad & \text{iff} \qquad \frac{1}{1+x_1} = \frac{1}{1+x_2} \\ & \text{iff} \qquad 1 + x_1 = 1 + x_2 \\ & \text{iff} \qquad x_1 = x_2 \end{aligned}$$

In particular, $f(x_1) = f(x_2)$ implies $x_1 = x_2$ for all $x_1, x_2 \in \mathbb{R}^+$, which proves that f is one-to-one.

Step 2. (f is onto.) Let $y = \frac{1}{1+x}$. Solving for x in terms of y we obtain

$$x = \frac{1}{y} - 1.$$

Note that if $0 < y < 1$, then

$$x = \frac{1}{y} - 1 > \frac{1}{1} - 1 = 0.$$

Therefore, for all $y \in (0, 1)$, there exists $x \in \mathbb{R}^+$, namely $x = \frac{1}{y} - 1$, such that

$$f(x) = \frac{1}{1+x} = \frac{1}{1 + (\frac{1}{y} - 1)} = \frac{1}{\frac{1}{y}} = y$$

This proves f is onto.

Therefore, f is a bijection.

Image and Preimage

If $f : A \to B$ and $S \subseteq A$, then the **image** of S under f is the set

$$f(S) = \{b \in B \mid b = f(s) \text{ for some } s \in S\}$$

If $T \subseteq B$, then the **preimage** of T is the set

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

$x \in f^{-1}(T)$ iff $f(x) \in T$

Image and Preimage

Example: Consider the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$.

- codomain of f:
- range of f:
- If $S = [-2, 3)$, then $f(S) =$
- If $T = (-1, 4]$, then $f^{-1}(T) =$

Image and Preimage

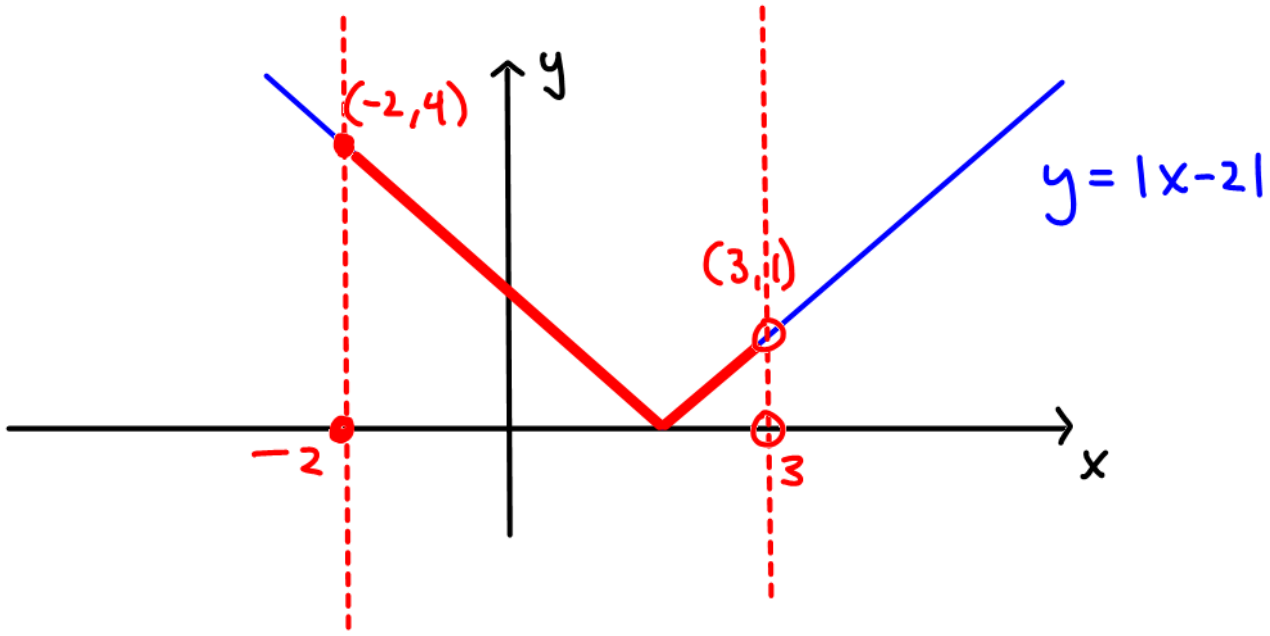
Example: Consider the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$.

- codomain of f: $\mathbb{R}$
- range of f: $[0, \infty)$
- If $S = [-2, 3)$, then $f(S) = [0, 9)$
- If $T = (-1, 4]$, then $f^{-1}(T) = [-2, 2]$

Image and Preimage

Example: Consider the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = |x - 2|$.

(a) Let $S = [-2, 3)$. Find $f(S)$.



(b) Let $T = (-1, 4]$. Find $f^{-1}(T)$.

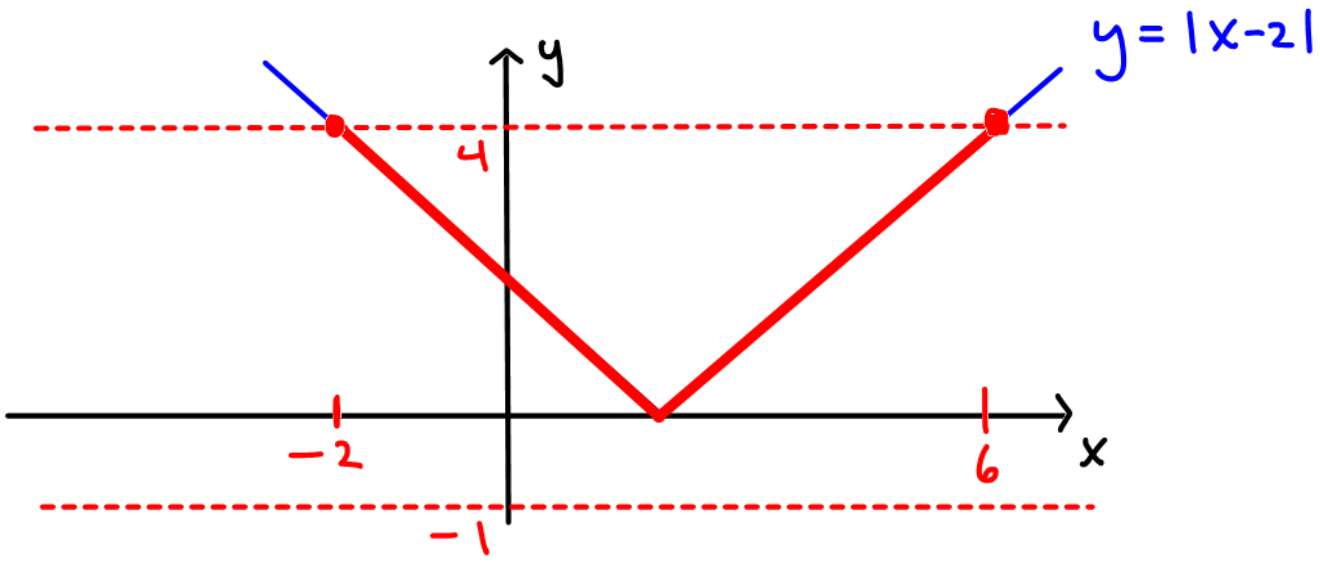


Image and Preimage

Let $f : A \to B$, where A and B are nonempty sets. Prove that if $S_1, S_2 \subseteq A$, then

$$f(S_1 \cup S_2) = f(S_1) \cup f(S_2).$$

Proof: First assume $y \in f(S_1 \cup S_2)$. Then, there exists an element $s \in S_1 \cup S_2$ such that $y = f(s)$. Therefore $y = f(s)$ for some $s \in S_1$, or $y = f(s)$ for some $s \in S_2$. That is, $y \in f(S_1)$ or $y \in f(S_2)$. Therefore, $y \in f(S_1) \cup f(S_2)$. This proves $f(S_1 \cup S_2) \subseteq f(S_1) \cup f(S_2)$.

Conversely, assume $y \in f(S_1) \cup f(S_2)$. Then, $y \in f(S_1)$ or $y \in f(S_2)$. Therefore, $y = f(s)$ for some $s \in S_1$, or $y = f(s)$ for some $s \in S_2$. Therefore, there exists $s \in S_1 \cup S_2$ such that $y = f(s)$. This proves $f(S_1) \cup f(S_2) \subseteq f(S_1 \cup S_2)$.

Therefore, $f(S_1) \cup f(S_2) = f(S_1 \cup S_2)$.

Image and Preimage

Let $f : A \to B$, where A and B are nonempty sets. Prove that if $T_1, T_2 \subseteq B$, then

$$f^{-1}(T_1 \cap T_2) = f^{-1}(T_1) \cap f^{-1}(T_2)$$

Proof: For all $a \in A$, we have

$a \in f^{-1}(T_1 \cap T_2)$ iff $f(a) \in T_1 \cap T_2$

iff $f(a) \in T_1$ and $f(a) \in T_2$

iff $a \in f^{-1}(T_1)$ and $a \in f^{-1}(T_2)$

iff $a \in f^{-1}(T_1) \cap f^{-1}(T_2)$.

Therefore, $f^{-1}(T_1 \cap T_2) = f^{-1}(T_1) \cap f^{-1}(T_2)$.

Identity Function

Let A be a set. The **identity function** on A is the function $i_A : A \to A$ defined by

$$i_A(x) = x$$

for all $x \in A$. That is,

$$i_A = \{(x, x) \mid x \in A\}.$$

The identity function i_A is one-to-one and onto, so it is a bijection.

Inverse Function

Let $f : A \to B$ be a bijection. The **inverse function** of f, denoted by f^{-1}, is the function that assigns to an element $b \in B$ the unique element $a \in A$ such that $f(a) = b$. That is,

$$f^{-1}(b) = a \quad \text{if and only if} \quad f(a) = b$$

If f has an inverse function, we say that f is **invertible**.

Note that we use the notation $f^{-1}(T)$ to denote the preimage of a set $T \subseteq B$, even when f is not invertible.

Examples

Let $A = \{1, 2, 3, 4\}$, $B = \{a, b, c\}$, $C = \{\alpha, \beta, \gamma\}$.

Determine if each function invertible. If so, find f^{-1}.

1. $f : B \to C$ defined by $\begin{cases} f(a) = \beta \\ f(b) = \gamma \\ f(c) = \alpha \end{cases}$

2. $f : A \to B$ defined by $\begin{cases} f(1) = a \\ f(2) = b \\ f(3) = a \\ f(4) = b \end{cases}$

Example

Determine if each function invertible. If so, find f^{-1}.

1. $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = n + 1$

2. $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 2x + 3$

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

Functions with Restricted Domains

If $f : A \to B$ is a function, and $D \subseteq A$, then the **restriction of f to D**, denoted $f\big|_D$ is the function

$$f\big|_D = \Big\{(x, y) \in f \;\; | \;\; x \in D\Big\}.$$

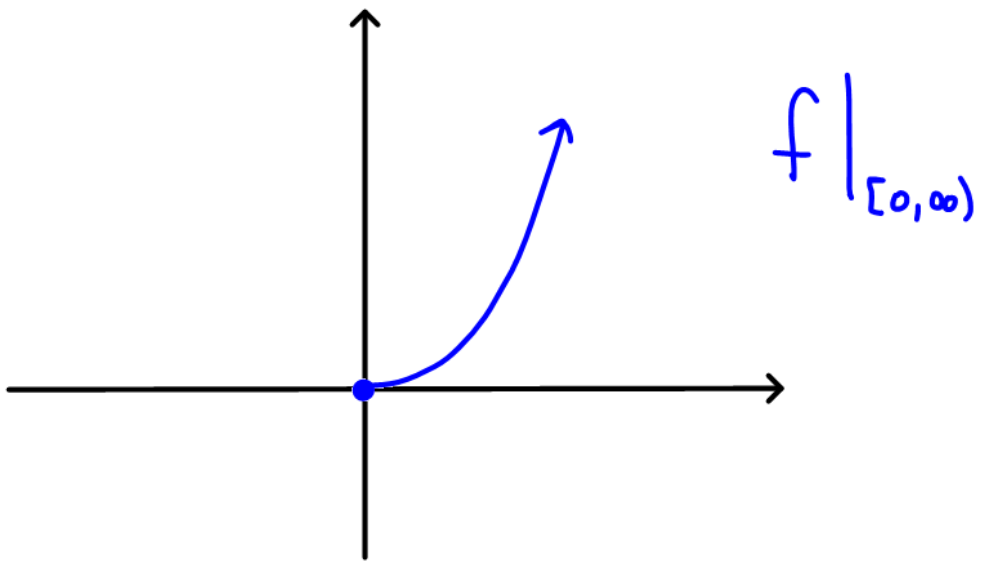
If g and h are functions and g is a restriction of h, we say h is an **extension** of g.

Functions with Restricted Domains

Example: Let $f : \mathbb{R} \to \mathbb{R}$ be the function defined by $f(x) = x^2$. If $D = [0, \infty)$, then

$$f\Big|_D = \Big\{(x, y) \in \mathbb{R} \times \mathbb{R} \;\Big|\; y = x^2 \text{ and } x \geq 0\Big\}.$$

The graph of $f\Big|_D$ is shown below.

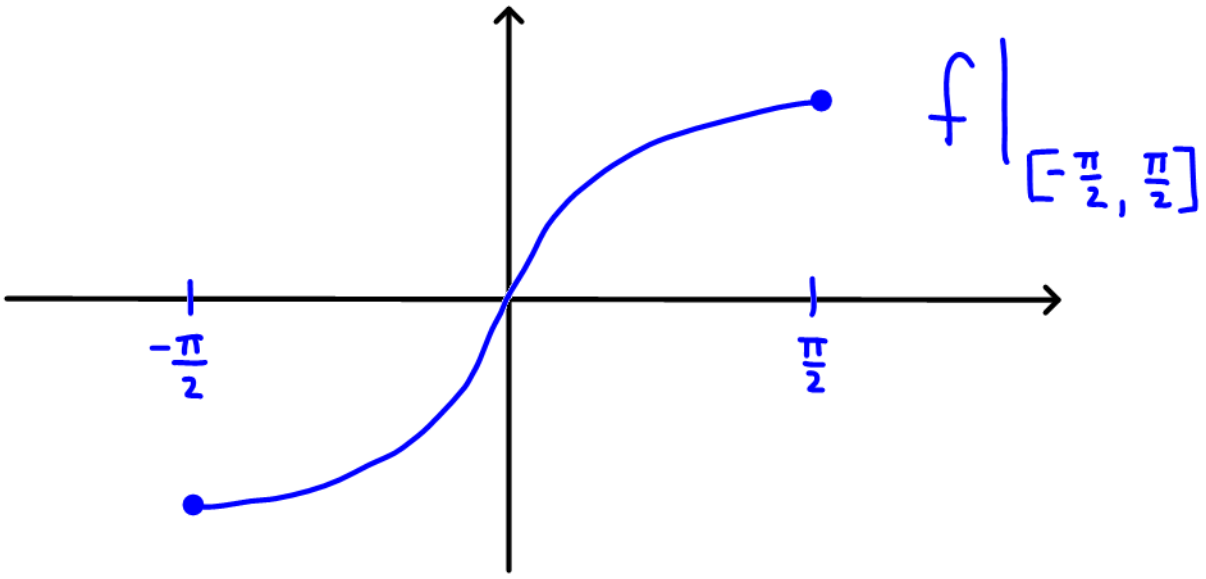


Functions with Restricted Domains

Example: Let $f : \mathbb{R} \to \mathbb{R}$ be the function defined by $f(x) = \sin(x)$. If $D = [-\frac{\pi}{2}, \frac{\pi}{2}]$, then $f|_D$ is given by

$$\left\{(x, y) \in \mathbb{R}\times\mathbb{R} \mid y = \sin(x) \text{ and } -\frac{\pi}{2} \leq x \leq \frac{\pi}{2}\right\}.$$

The graph of $f\Big|_D$ is shown below.



(The inverse function of $f|_{[-\frac{\pi}{2}, \frac{\pi}{2}]}$ is $\sin^{-1}(x)$)

Piecewise-Defined Functions

If $f_1 : A_1 \to B_1$ and $f_2 : A_2 \to B_2$ are functions, and $A_1 \cap A_2 = \emptyset$, then the function $f : A_1 \cup A_2 \to B_1 \cup B_2$ defined by

$$f(x) = \begin{cases} f_1(x) & \text{if } x \in A_1, \\ f_2(x) & \text{if } x \in A_2. \end{cases}$$

is called a **piecewise-defined function**.

As a set of ordered pairs, note that

$$f = f_1 \cup f_2.$$

Piecewise-Defined Functions

Example: $f(x) = |x|$

The **absolute value function**, denoted by $f(x) = |x|$ is the piecewise defined function

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

In other words,

$$f(x) = \begin{cases} f_1(x) & \text{if } x \in [0, \infty), \\ f_2(x) & \text{if } x \in (-\infty, 0). \end{cases}$$

where $f_1 : [0, \infty) \to \mathbb{R}$ and $f_2 : (-\infty, 0) \to \mathbb{R}$ are defined by $f_1(x) = x$ and $f_2(x) = -x$.

Characteristic Functions

Let U be the universal set, and let $A \subseteq U$. Then, $\chi_A : U \to \mathbb{R}$, defined by

$$\chi_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \in U - A \end{cases}$$

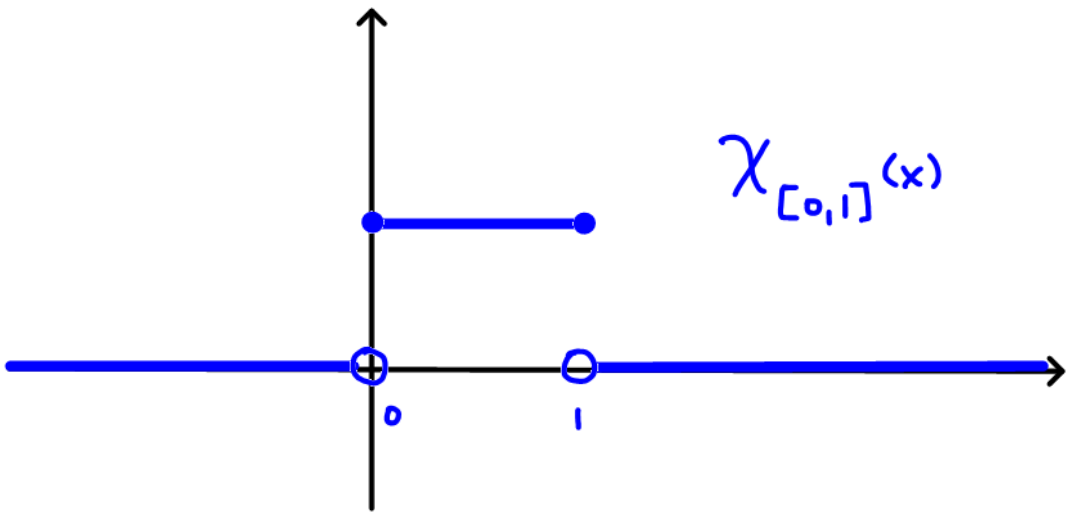
is called the **characteristic function on A**.

Characteristic Functions

Example

Let $U = \mathbb{R}$ and let $A = [0, 1]$. Then, $\chi_{[0,1]} : \mathbb{R} \to \mathbb{R}$, is given by

$$\chi_{[0,1]}(x) = \begin{cases} 1 & \text{if } x \in [0, 1] \\ 0 & \text{otherwise} \end{cases}$$



Piecewise-Defined Functions

More generally, if

$$\mathcal{F} = \{f_\alpha : A_\alpha \to B_\alpha \mid \alpha \in \Delta\}$$

is a family of functions with pairwise disjoint domains $\{A_\alpha \mid \alpha \in \Delta\}$, then

$$f = \bigcup_{\alpha \in \Delta} f_\alpha$$

is the piecewise-defined function

$$f(x) = f_\alpha(x) \quad \text{iff} \quad x \in A_\alpha.$$

Piecewise-Defined Functions

Example $f(x) = \lfloor x \rfloor$

Let $A_k = [k, k+1)$ for each $k \in \mathbb{Z}$, and let $f_k : A_k \to \mathbb{R}$ be the constant function

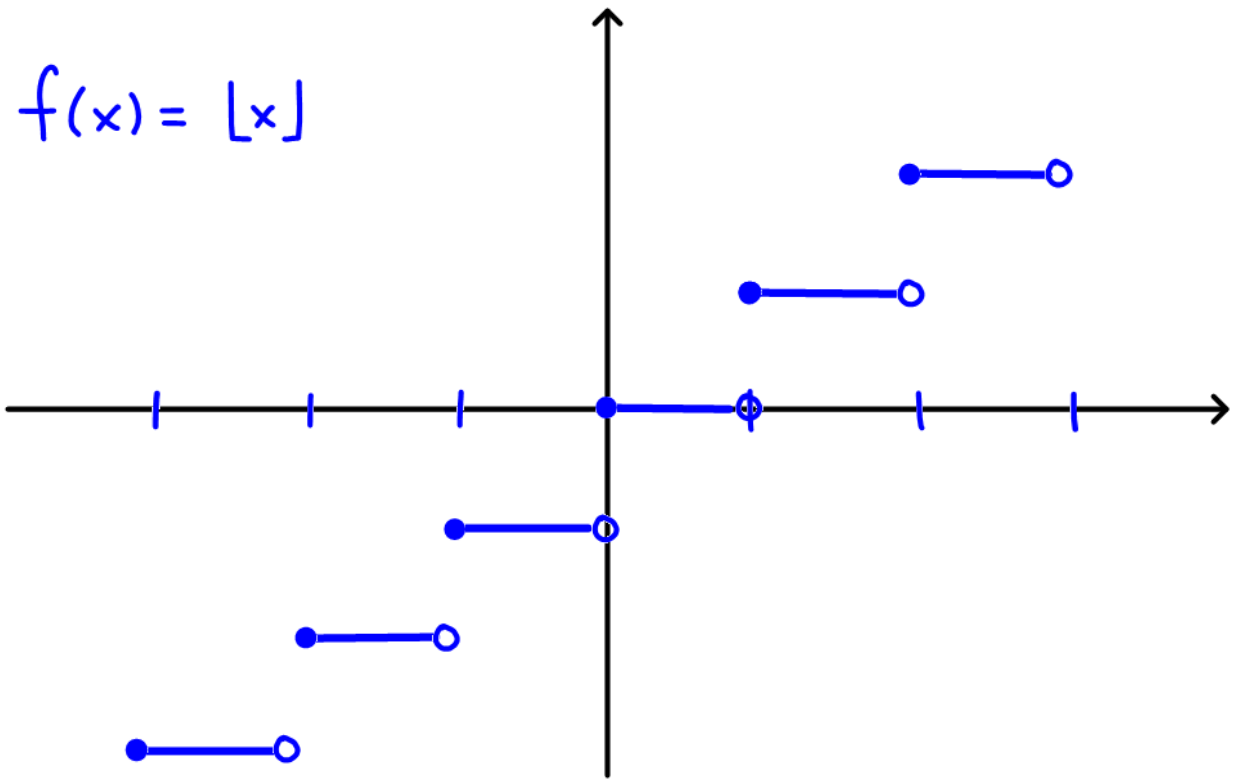
$$f_k(x) = k.$$

Then, the **greatest integer function** or **floor function**, denoted $f(x) = \lfloor x \rfloor$ is the piecewise defined function

$$f = \bigcup_{k \in \mathbb{Z}} f_k$$

That is,

$$\lfloor x \rfloor = k \quad \text{iff} \quad x \in A_k.$$


f(x) = ⌊x⌋

Sequence

Let S be a set. A **sequence** with values in S is a function $s : \mathbb{Z}^+ \to S$. If $n \in \mathbb{Z}^+$, then $s(n) \in S$ represents the nth term in the sequence, which we denote by s_n.

Sequence

Example

Let $S = \mathbb{R}$, and let $s : \mathbb{Z}^+ \to S$ be the function defined by $s(n) = 2^{-n}$. Then s corresponds to the sequence

$$s_1 = \frac{1}{2},$$

$$s_2 = \frac{1}{4},$$

$$s_3 = \frac{1}{8},$$

$$s_4 = \frac{1}{16},$$

$$s_5 = \frac{1}{32},$$

$$\vdots$$

Cardinality of Sets

Cardinality

We say the sets A and B have the same **cardinality** if and only if there is a one-to-one correspondence (bijection) from A to B. When A and B have the same cardinality, we write $|A| = |B|$.

Cardinality

If there is a one-to-one function from A to B, the cardinality of A is less than or the same as the cardinality of B and we write $|A| \leq |B|$. Moreover, when $|A| \leq |B|$ and A and B have different cardinality, we say that the cardinality of A is less than the cardinality of B and we write $|A| < |B|$.

Countable Set

A set that is either finite or has the same cardinality as the set of positive integers $\mathbb{Z}^+$ is called **countable**. A set that is not countable is called **uncountable**.

When an infinite set S is countable, we denote the cardinality of S by $\aleph_0$ (where $\aleph$ is aleph, the first letter of the Hebrew alphabet). We write $|S| = \aleph_0$ and say that S has cardinality **aleph null**.

Countable Set

Example: Prove the set of odd positive integers is a countable set.

Solution: Let $O = \{1, 3, 5, \ldots\}$ be the set of odd positive integers. To show O is countable we must find a bijection from $\mathbb{Z}^+$ to O.

The function $f : \mathbb{Z}^+ \to O$ defined by

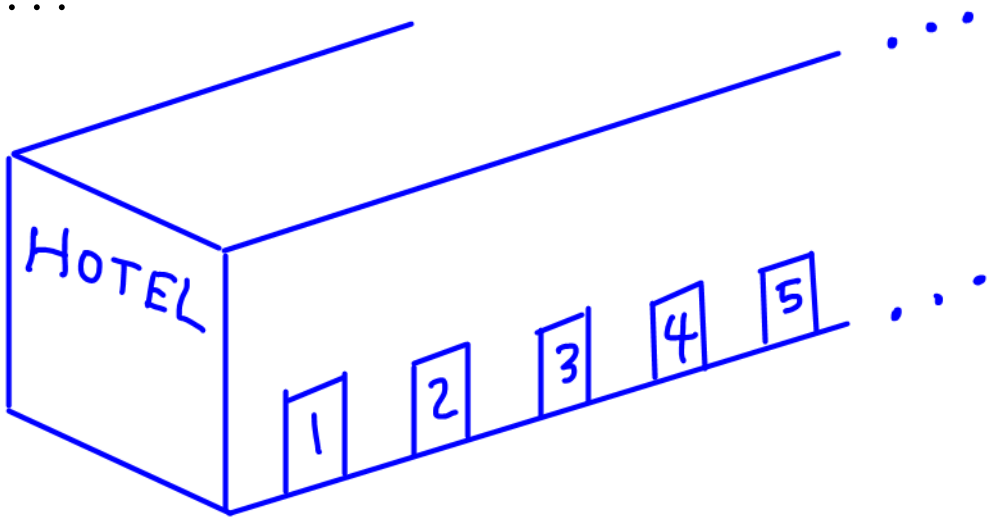
$$f(n) = 2n - 1$$

is a bijection. Hence O is a countable set.

Countable Set

Hilbert's Grand Hotel

Consider a "Grand Hotel" , which has a countably infinite number of rooms, numbered $1, 2, 3, \ldots$



Question: How can we accommodate a new guest arriving at a fully occupied Grand Hotel without removing any of the current guests?

Countable Set

Hilbert's Grand Hotel

Question: How can we accommodate a new guest arriving at a fully occupied Grand Hotel without removing any of the current guests?

Solution: Because the rooms of the Grand Hotel are countable, we can list them as Room 1, Room 2, Room 3, and so on. When a new guest arrives, we move the guest in Room 1 to Room 2, the guest in Room 2 to Room 3, and in general, the guest in Room n to Room $n+1$, for all positive integers n. This frees up Room 1, which we assign to the new guest, and all the current guests still have rooms.

Countable Set

Hilbert's Grand Hotel

Equivalent problem: Show that the union of countable set and a singleton set is countable.

Solution: Let A be a countable set. Then, there is a bijective function $f : \mathbb{Z}^+ \to A$. Let $A = \{a_1, a_2, a_3, \ldots\}$ where we define $a_n = f(n)$ for all $n \in \mathbb{Z}^+$.

Let the singleton set be represented by $\{a_0\}$. Then, the function $g : \mathbb{Z}^+ \to A \cup \{a_0\}$ defined by $g(n) = a_{n-1}$ is a bijection, which shows that $A \cup \{a_0\}$ is countable.

(To relate this problem to the previous one, think of A as the set of hotel guests and a_0 as the new guest. Then, prior to the arrival of a_0, $f(n) = a_n$ means room n is occupied by guest a_n.)

Countable Set

Example: Prove the set of integers is countable.

Solution: Consider the function $f : \mathbb{Z}^+ \to \mathbb{Z}$ defined by

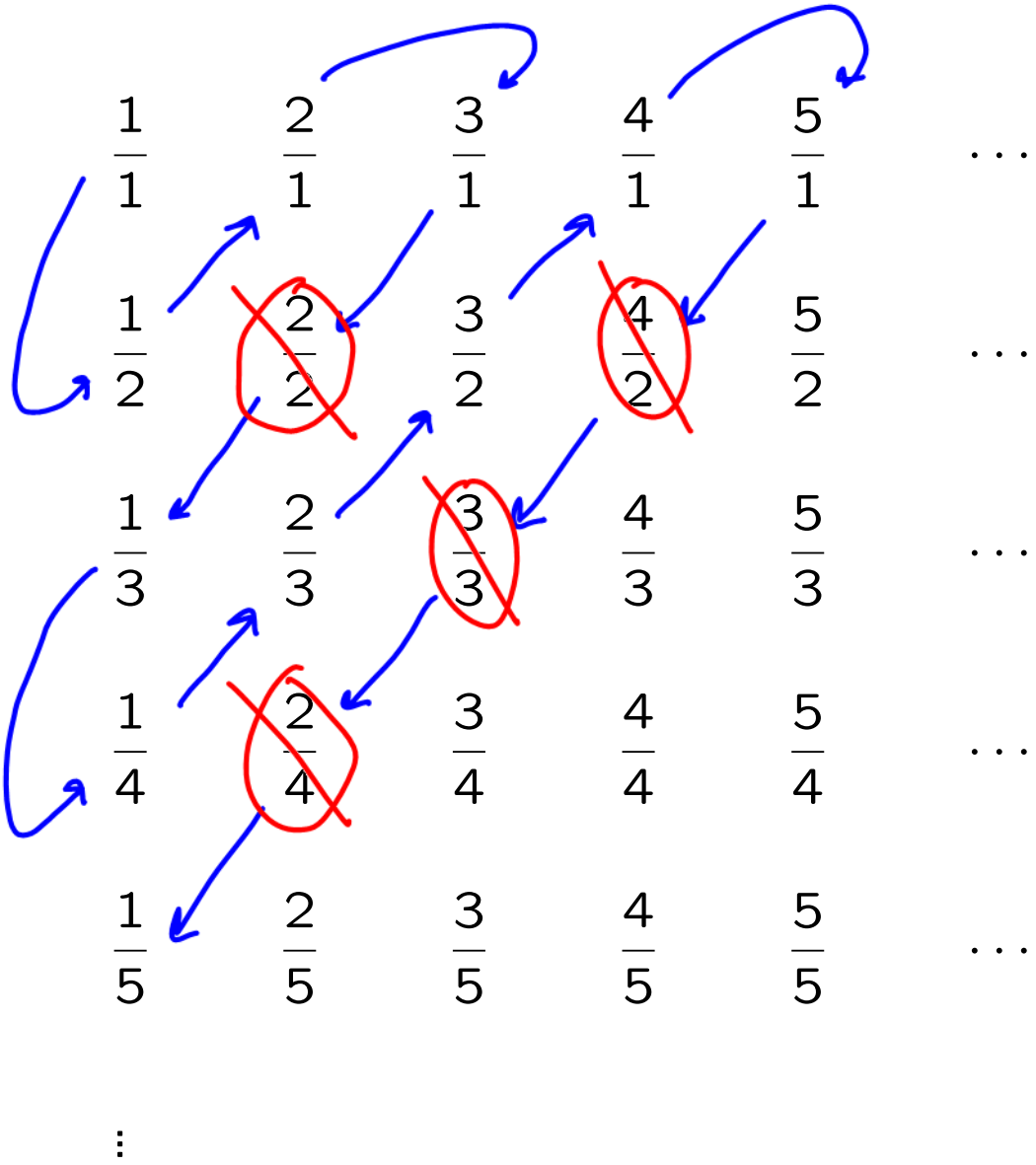
$$f(n) = \begin{cases} \dfrac{n}{2} & \text{if n is even} \\ -\dfrac{(n-1)}{2} & \text{if n is odd} \end{cases}$$

Since f is a bijection, this shows that the set $\mathbb{Z}$ is countable.

Countable Set

Example: Prove the set of positive rational numbers is countable.

Solution: While we will not give an explicit bijective function from $\mathbb{Z}^+$ to $\mathbb{Q}^+$, we will show how to list the positive rationals as a sequence $\{r_1, r_2, r_3, \ldots\}$. First we arrange the rationals in an infinite grid as shown below, where the ith row contains the sequence $\{\frac{1}{i}, \frac{2}{i}, \frac{3}{i}, \ldots\}$


1/1 2/1 3/1 4/1 5/1 ...
1/2 2/2 3/2 4/2 5/2 ...
1/3 2/3 3/3 4/3 5/3 ...
1/4 2/4 3/4 4/4 5/4 ...
1/5 2/5 3/5 4/5 5/5 ...
⋮

We first list the positive rational numbers p/q with $p+q=2$, followed by those with $p+q=3$, followed by those with $p+q=4$, and so on, following the path shown above. Whenever we encounter a number p/q that is already listed (e.g. 2/2), we do not list it again.

Since $\mathbb{Q}^+$ can be represented as a sequence, it is a countable set.

Uncountable Set

Example: Prove the set of real numbers is uncountable.

Solution: The proof relies on a **Cantor diagonalization argument**. Assume for the sake of contradiction that $\mathbb{R}$ is countable. Then, the subset $(0, 1)$ must also be countable and can be represented as sequence of numbers

$$
\begin{aligned}
r_1 &= 0.\, d_{11}\, d_{12}\, d_{13}\, d_{14} \ldots \\
r_2 &= 0.\, d_{21}\, d_{22}\, d_{23}\, d_{24} \ldots \\
r_3 &= 0.\, d_{31}\, d_{32}\, d_{33}\, d_{34} \ldots \\
r_4 &= 0.\, d_{41}\, d_{42}\, d_{43}\, d_{44} \ldots \\
&\vdots
\end{aligned}
$$

Then, form a new real number with decimal expansion $r = 0.d_1\, d_2\, d_3\, d_4 \ldots$, where the decimal digits are determined by the following rule:

$$d_i = \begin{cases} 4 & \text{if } d_{ii} \neq 4 \\ 5 & \text{if } d_{ii} = 4 \end{cases}$$

Therefore, the real number r is not equal to any of the numbers $\{r_1, r_2, r_3, \ldots\}$ because the decimal expansion of r differs from the decimal expansion of r_i in the ith place to the right of the decimal point, for each i.

Because there is a real number r between 0 and 1 that is not in the list, the assumption that all the real numbers between 0 and 1 could be listed must be false. Therefore, all the real numbers between 0 and 1 cannot be listed, so the set of real numbers between 0 and 1 is uncountable.

Countable Set

Theorem: If A and B are countable sets, then $A \cup B$ is also countable.

Countable Set

Example: Prove the set of positive integers not divisible by 4 is a countable set.