# MATHD022: Discrete Mathematics

Connor Petri

Spring 2025

# Contents

# 1. The Language of Mathematics

---

## 1.1 Variables

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

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

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

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

**Types of Statements**

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

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

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

- A **universal existential statement** is a statement where the first part is universal and the second part is existential.
  - **Every** real number **has** an additive inverse.
  - **For all** real numbers $r$, **there is** an additive inverse $-r$.
  - **For all** real numbers $r$, **there is** a real number $s$ such that $r+s=0$.

- An **existential universal statement** is a statement where the first part is existential and the second part is universal.
  - **There is** a positive integer that is less than or equal to **every** positive integer.
  - **There is** a positive intefer $m$ such that **every** positive integer is greater than or equal to $m$.
  - **There is** a positive integer $m$ with the property that **for all** positive integers $n$, $m \leq n$.

## 1.2 Sets

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

**Notation**

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

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

**Common Sets**

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

  The null set is a subset of every set.

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

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

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

## Subsets

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

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

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

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

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

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

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

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

## 1.3 Relations and Functions

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

$$R \subseteq A \times B$$

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

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

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

### Functions

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

- For every element $x \in A$, there is an element $y \in B$ such $(x, y) \in F$
- For every element $x \in A$,

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

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

## Equivalent Functions

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

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

# 2. The Logic of Compound Statements

## 2.1 Logical Form and Equivalence

---

### Arguments

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

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

**Example**

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

### Logical Statements

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

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

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

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

## Equivalent Statements

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

$$p \equiv q$$

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

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

**Tautological and Condtradictory Statements**

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

## 2.2 Conditional Statements

---

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

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

**Order of Operations**

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

**Equivalent of Conditional Statements**

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

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

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

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

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

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

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

**More statement types**

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

**Example** If today is Easter then tomorrow is Monday.

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

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

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

**Sufficient and Necessary Conditions** If $r$ and $s$ are statements:

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

## 2.3 Valid and Invalid Arguments

---

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

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

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

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

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

Therefore the argument form is invalid.

## Syllogisms

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

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

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

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

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

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

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

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

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

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

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

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

## Contradictions

**Definition** A contradiction is a statement that is always false.

$$\neg p \implies c$$
$$\therefore p$$

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

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

---

Suppose A is a knight:

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

# 3. The Logic of Quantified Statements

## 3.1 Predicates and Quantified Statements (Part 1)

---

### Predicates

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

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

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

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

### Truth Sets

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

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

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

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

# Quantified Statements

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

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

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

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

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

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

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

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

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

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

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

## 3.2 Predicates and Quantified Statements (Part 2)

---

### Negations of Quantified Statements

**Negation of a Universal Statement**

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

**Negation of an Existential Statement**

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

**Negation of a Universal Conditional Statement**

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

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

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

## 3.3 Statements with Multiple Quantifiers

---

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

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

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

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

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

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

**Negation of Multiply-Quantified Statements**

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

## 3.4 Arguments with Quantified Statements

---

### Universal Model Ponens (Direct Proof)

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

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

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

### Universal Modus Tollens (Prove by Contradiction)

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

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

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

### Converse and Inverse Errors

**Converse Error**

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

**Inverse Error**

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

# 4. Elementary Number Theory and Methods of Proof

## 4.1 Direct Proof and Counterexample

---

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

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

**Example** Is -301 even or odd?

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

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

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

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

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

Constructive Proof of Existential Statement

$$\exists x in D \ni Q(x)$$

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

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

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

## Disproving Universal Statement by Counterexample

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

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

## Method of Exhaustion of Proving Universal Statement

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

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

## Direct Proof of Universal Statement

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

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

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

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

## 4.2 Skipped

## 4.3 Rational Numbers

---

**Definitions**

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

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

First we rewrite 320.5 as a fraction:

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

Then we rewrite 0.0492492... as a fraction:

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

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

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

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

Now we can combine the two fractions:

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

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

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

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

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

$$\therefore \quad 320.5492492... \text{ is rational.}$$

## Zero Product Property

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

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

**Example**

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

## Corollaries

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

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

Let $a, b \in \mathbb{Q}$ :

$\therefore \quad a = \dfrac{n}{m}, \exists n, m \in \mathbb{Z} \wedge m \neq 0$ Definition of rational numbers.

$\therefore \quad b = \dfrac{s}{t}, \exists s, t \in \mathbb{Z} \wedge t \neq 0$

$\therefore \quad a \cdot b = \dfrac{n}{m} \cdot \dfrac{s}{t}, m \neq 0 \wedge t \neq 0$

$\therefore \quad ab = \dfrac{ns}{mt}, mt \neq 0$ Zero product property.

$\therefore \quad ab \in \mathbb{Q}$

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

$\forall p, q \in \mathbb{Q}, \dfrac{p}{q} \in \mathbb{Q}$ Statement

Let $p = 1, q = 0$

$\therefore \quad \dfrac{p}{q} \notin \mathbb{Q}$

$\therefore \quad \exists p, q \in \mathbb{Q} \ni \dfrac{p}{q} \notin \mathbb{Q}$

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

$\therefore \quad a < b \implies a + b < 2b$

$\because \quad \dfrac{1}{2} > 0$

$\therefore \quad a < b \wedge \dfrac{1}{2} > 0 \implies \dfrac{a+b}{2} < \dfrac{b}{2}$

$\therefore \quad a < b \implies 2a < b + a$

$\because \quad \dfrac{1}{2} > 0$

$\therefore \quad a < b \wedge \dfrac{1}{2} > 0 \implies a < \dfrac{a+b}{2}$

$\therefore \quad a < \dfrac{a+b}{2} \wedge \dfrac{a+b}{2} < b \equiv a < \dfrac{a+b}{2} < b$

## 4.4 Divisibility

---

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

- Notation: $d|n$ is read "d divides n".
  - $d|n \iff \exists k \in \mathbb{Z} \ni n = dk$

It is equivalent to the following statements:

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

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

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

### Divisibility Theorems

**Positive Divisor of a Positive Integer Theorem**

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

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

**Transistivity of Divisibility Theorem**

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

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

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

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

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

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

## 4.5 The Quotient-Remainder Theorem

**Theorem**

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

**Definition** Given any integer n and any positive integer d:

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

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

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

### The Parity Property

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

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

**Example** The product of two consecutive integers is even.

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

Case 1: $n$ is even

$\therefore \quad n = 2k, \exists k \in \mathbb{Z}$

$\therefore \quad n + 1 = 2k + 1$

$\therefore \quad n(n+1) = 2k(2k+1) =$

$\therefore \quad n(n+1) = 2(2k^2 + k)$

$\therefore \quad n(n+1)$ is even

Case 2: $n$ is odd

$\therefore \quad n = 2k + 1, \exists k \in \mathbb{Z}$

$\therefore \quad n + 1 = 2k + 2$

$\therefore \quad n(n+1) = (2k+1)(2k+2) \therefore \qquad n(n+1) = 2((k+1)(2k+1))$

$\therefore \quad n(n+1)$ is even

## Absolute Value

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

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

**Lemma**

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

**The Triangle Inequality**

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

## 4.6 Skipped

## 4.7 Contradiction and Contraposition

---

### Method of Proof by Contradiction

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

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

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

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

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

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

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

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

## Method of Proof by Contraposition

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

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

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

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