**Definition 2.1.1 (Statement)**

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

**Definition 2.1.2 (Negation)**

If $p$ is a statement variable, the **negation** of $p$ is "not $p$" or "it is not the case that $p$" and is denoted $\sim p$.

**Definition 2.1.3 (Conjunction)**

If $p$ and $q$ are statement variables, the **conjunction** of $p$ and $q$ is "$p$ and $q$", denoted $p \wedge q$.

**Definition 2.1.4 (Disjunction)**

If $p$ and $q$ are statement variables, the **disjunction** of $p$ and $q$ is "$p$ or $q$", denoted $p \vee q$.

**Definition 2.1.5 (Statement Form/Propositional Form)**

A **statement form** (or **propositional form**) is an expression made up of statement variables and logical connectives that becomes a statement when actual statements are substituted for the component statement variables.

**Definition 2.1.6 (Logical Equivalence)**

Two statement forms are called **logically equivalent** if, and only if, they have identical truth values for each possible substitution of statements for their statement variables.

The logical equivalence of statement forms $P$ and $Q$ is denoted by $P \equiv Q$.

**Definition 2.1.7 (Tautology)**

A **tautology** is a statement form that is always true regardless of the truth values of the individual statements substituted for its statement variables. A statement whose form is a tautology is a **tautological statement**.

**Definition 2.1.8 (Contradiction)**

A **contradiction** is a statement form that is always false regardless of the truth values of the individual statements substituted for its statement variables. A statement whose form is a contradiction is a **contradictory statement**.

**Definition 2.2.1 (Conditional)**

If $p$ and $q$ are statement variables, the **conditional** of $q$ by $p$ is "if $p$ then $q$" or "$p$ implies $q$", denoted $p \to q$.
It is false when $p$ is true and $q$ is false; otherwise it is true.
We called $p$ the hypothesis (or antecedent) and $q$ the conclusion (or consequent).

**Definition 2.2.2 (Contrapositive)**

The **contrapositive** of a conditional statement "if $p$ then $q$" is "if $\sim q$ then $\sim p$".
Symbolically, the contrapositive of $p \to q$ is $\sim q \to \sim p$.

**Definition 2.2.3 (Converse)**

The **converse** of a conditional statement "if $p$ then $q$" is "if $q$ then $p$".
Symbolically, the converse of $p \to q$ is $q \to p$.

**Definition 2.2.4 (Inverse)**

The **inverse** of a conditional statement "if $p$ then $q$" is "if $\sim p$ then $\sim q$".
Symbolically, the inverse of $p \to q$ is $\sim p \to \sim q$.

**Definition 2.2.5 (Only If)**

If $p$ and $q$ are statements,
"$p$ only if $q$" means "if not $q$ then not $p$"
Or, equivalently,
"if $p$ then $q$"

**Definition 2.2.6 (Biconditional)**

Given statement variables $p$ and $q$, the **biconditional** of $p$ and $q$ is "$p$ if, and only if, $q$" and is denoted $p \leftrightarrow q$.

It is true if both $p$ and $q$ have the same truth values and is false if $p$ and q have opposite truth values.

The words *if and only if* are sometimes abbreviated *iff*.

**Definition 2.2.7 (Necessary and Sufficient Conditions)**

If $r$ and $s$ are statements,
"$r$ is a sufficient condition for $s$" means "if $r$ then $s$"
"$r$ is a necessary condition for $s$" means "if not $r$ then not $s$" (or "if $s$ then $r$")

**Definition 2.3.1 (Argument)**

An **argument** (**argument form**) is a sequence of statements (statement forms). All statements in an argument (argument form), except for the final one, are called **premises** (or **assumptions** or **hypothesis**). The final statement (statement form) is called the **conclusion**. The symbol •, which is read "therefore", is normally placed just before the conclusion.

To say that an argument form is **valid** means that no matter what particular statements are substituted for the statement variables in its premises, if the resulting premises are all true, then the conclusion is also true.

**Definition 2.3.2 (Sound and Unsound Arguments)**

An argument is called **sound** if, and only if, it is valid and all its premises are true.

An argument that is not sound is called **unsound**.

**Theorem 2.1.1 Logical Equivalences**

Given any statement variables $p$, $q$ and $r$, a tautology **true** and a contradiction **false**:

| | | | |
|---|---|---|---|
| 1 | Commutative laws | $p \wedge q \equiv q \wedge p$ | $p \vee q \equiv q \vee p$ |
| 2 | Associative laws | $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ | $(p \vee q) \vee r \equiv p \vee (q \vee r)$ |
| 3 | Distributive laws | $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ | $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ |
| 4 | Identity laws | $p \wedge \mathbf{true} \equiv p$ | $p \vee \mathbf{false} \equiv p$ |
| 5 | Negation laws | $p \vee \sim p \equiv \mathbf{true}$ | $p \wedge \sim p \equiv \mathbf{false}$ |
| 6 | Double negative law | $\sim(\sim p) \equiv p$ | |
| 7 | Idempotent laws | $p \wedge p \equiv p$ | $p \vee p \equiv p$ |
| 8 | Universal bound laws | $p \vee \mathbf{true} \equiv \mathbf{true}$ | $p \wedge \mathbf{false} \equiv \mathbf{false}$ |
| 9 | De Morgan's laws | $\sim(p \wedge q) \equiv \sim p \vee \sim q$ | $\sim(p \vee q) \equiv \sim p \wedge \sim q$ |
| 10 | Absorption laws | $p \vee (p \wedge q) \equiv p$ | $p \wedge (p \vee q) \equiv p$ |
| 11 | Negation of **true** and **false** | $\sim\mathbf{true} \equiv \mathbf{false}$ | $\sim\mathbf{false} \equiv \mathbf{true}$ |

*: Note that there is no ambiguity in $p \wedge q \wedge r$ as it is equivalent to $(p \wedge q) \wedge r$ and $p \wedge (q \wedge r)$. Likewise for $\vee$.



| Rule of inference | |
|---|---|
| Modus Ponens | $p \to q$<br>$p$<br>• $q$ |
| Modus Tollens | $p \to q$<br>$\sim q$<br>• $\sim p$ |
| Generalization | $p$<br>• $p \vee q$ |
| | $q$<br>• $p \vee q$ |
| Specialization | $p \wedge q$<br>• $p$ |
| | $p \wedge q$<br>• $q$ |
| Conjunction | $p$<br>$q$<br>• $p \wedge q$ |

| Rule of inference | |
|---|---|
| Elimination | $p \vee q$<br>$\sim q$<br>• $p$ |
| | $p \vee q$<br>$\sim p$<br>• $q$ |
| Transitivity | $p \to q$<br>$q \to r$<br>• $p \to r$ |
| Proof by Division Into Cases | $p \vee q$<br>$p \to r$<br>$q \to r$<br>• $r$ |
| Contradiction Rule | $\sim p \to \mathbf{false}$<br>• $p$ |

### Definition 3.1.1 (Predicate)

A **predicate** is a sentence that contains a finite number of variables and becomes a statement when specific values are substituted for the variables.
The **domain** of a predicate variable is the set of all values that may be substituted in place of the variable.

### Definition 3.1.2 (Truth set)

If $P(x)$ is a predicate and $x$ has domain $D$, the **truth set** is the set of all elements of $D$ that make $P(x)$ true when they are substituted for x.
The truth set of $P(x)$ is denoted $\{x \in D \mid P(x)\}$.

### Definition 3.1.3 (Universal Statement)

Let $Q(x)$ be a predicate and $D$ the domain of $x$.
A **universal statement** is a statement of the form "$\forall x \in D$, $Q(x)$".

- It is defined to be true iff $Q(x)$ is true for every $x$ in $D$.
- It is defined to be false iff $Q(x)$ is false for at least one $x$ in $D$.

A value for $x$ for which $Q(x)$ is false is called a **counterexample.**

### Definition 3.1.4 (Existential Statement)

Let $Q(x)$ be a predicate and $D$ the domain of $x$.
An **existential statement** is a statement of the form "$\exists x \in D$ such that $Q(x)$".

- It is defined to be true iff $Q(x)$ is true for at least one $x$ in $D$.
- It is defined to be false iff $Q(x)$ is false for all $x$ in $D$.

$\exists!$ is the **uniqueness quantifier symbol**. It means "there exists a unique" or "there is one and only one".

### Definition 3.2.1 (Contrapositive, converse, inverse)

Consider a statement of the form: $\forall x \in D\ (P(x) \to Q(x))$.

1. Its **contrapositive** is: $\forall x \in D\ (\sim Q(x) \to \sim P(x))$.
2. Its **converse** is: $\forall x \in D\ (Q(x) \to P(x))$.
3. Its **inverse** is: $\forall x \in D\ (\sim P(x) \to \sim Q(x))$.

### Definition 3.2.2 (Necessary and Sufficient conditions, Only if)

- "$\forall x$, $r(x)$ is a **sufficient condition** for $s(x)$" means "$\forall x\ (r(x) \to s(x))$".
- "$\forall x$, $r(x)$ is a **necessary condition** for $s(x)$" means "$\forall x\ (\sim r(x) \to \sim s(x))$" or, equivalently, "$\forall x\ (s(x) \to r(x))$".
- "$\forall x$, $r(x)$ **only if** $s(x)$" means "$\forall x\ (\sim s(x) \to \sim r(x))$" or, equivalently, "$\forall x\ (r(x) \to s(x))$" .

### Definition 3.4.1 (Valid Argument Form)

To say that **an argument form is valid** means the following: No matter what particular predicates are substituted for the predicate symbols in its premises, if the resulting premise statements are all true, then the conclusion is also true.

An **argument is called valid** if, and only if, its form is valid.

## Definitions: Even and Odd Integers

An integer $n$ is even if, and only if, $n$ equals twice some integer.

An integer $n$ is odd if, and only if, $n$ equals twice some integer plus 1.

Symbolically, if $n$ is an integer, then

$n$ is even $\iff$ $\exists$ an integer $k$ such that $n = 2k$.
$n$ is odd $\iff$ $\exists$ an integer $k$ such that $n = 2k + 1$.

## Definitions: Prime and Composite

An integer $n$ is prime iff $n > 1$ and for all positive integers $r$ and $s$, if $n = rs$, then either $r$ or $s$ equals $n$.

An integer $n$ is composite iff $n > 1$ and $n = rs$ for some integers $r$ and $s$ with $1 < r < n$ and $1 < s < n$ .

In symbols:

$n$ is prime: $\forall r, s \in \mathbb{Z}^+$, if $n = rs$ then either $r = 1$ and $s = n$ or $r = n$ and $s = 1$.

$n$ is composite: $\exists\ r, s \in \mathbb{Z}^+$ s.t. $n = rs$ and $1 < r < n$ and $1 < s < n$.

### Theorem 3.2.1 Negation of a Universal Statement

The **negation** of a statement of the form

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

is logically equivalent to a statement of the form

$\exists x \in D$ such that $\sim P(x)$

Symbolically,

$\sim(\forall x \in D,\ P(x)) \equiv \exists x \in D$ such that $\sim P(x)$

### Theorem 3.2.2 Negation of an Existential Statement

The **negation** of a statement of the form

$\exists x \in D$ such that $P(x)$

is logically equivalent to a statement of the form

$\forall x \in D,\ \sim P(x)$

Symbolically,

$\sim(\exists x \in D$ such that $P(x)) \equiv \forall x \in D,\ \sim P(x)$

### Universal Modus Ponens

| *Formal version* | *Informal version* |
|---|---|
| $\forall x\ (P(x) \to Q(x))$. | If $x$ makes $P(x)$ true, then $x$ makes $Q(x)$ true. |
| $P(a)$ for a particular $a$. | $a$ makes $P(x)$ true. |
| • $Q(a)$. | • $a$ makes $Q(x)$ true. |

### Universal Modus Tollens

| *Formal version* | *Informal version* |
|---|---|
| $\forall x\ (P(x) \to Q(x))$. | If $x$ makes $P(x)$ true, then $x$ makes $Q(x)$ true. |
| $\sim Q(a)$ for a particular $a$. | $a$ does not make $Q(x)$ true. |
| • $\sim P(a)$. | • $a$ does not makes $P(x)$ true. |

### Converse Error (Quantified Form)

| *Formal version* | *Informal version* |
|---|---|
| $\forall x\ (P(x) \to Q(x))$. | If $x$ makes $P(x)$ true, then $x$ makes $Q(x)$ true. |
| $Q(a)$ for a particular $a$. | $a$ makes $Q(x)$ true. |
| • $P(a)$. | • $a$ makes $P(x)$ true. |

### Inverse Error (Quantified Form)

| *Formal version* | *Informal version* |
|---|---|
| $\forall x\ (P(x) \to Q(x))$. | If $x$ makes $P(x)$ true, then $x$ makes $Q(x)$ true. |
| $\sim P(a)$ for a particular $a$. | $a$ does not make $P(x)$ true. |
| • $\sim Q(a)$. | • $a$ does not make $Q(x)$ true. |

### Universal Transitivity

| *Formal version* | *Informal version* |
|---|---|
| $\forall x\ (P(x) \to Q(x))$. | Any $x$ that makes $P(x)$ true makes $Q(x)$ true. |
| $\forall x\ (Q(x) \to R(x))$. | Any $x$ that makes $Q(x)$ true makes $R(x)$ true. |
| • $\forall x\ (P(x) \to R(x))$. | • Any $x$ that makes $P(x)$ true makes $R(x)$ true. |

| Rule of Inference for quantified statements | Name |
|---|---|
| $\forall x \in D\ P(x)$<br>$\therefore P(a)$ if $a \in D$ | Universal instantiation |
| $P(a)$ for every $a \in D$<br>$\therefore \forall x \in D\ P(x)$ | Universal generalization |
| $\exists x \in D\ P(x)$<br>$\therefore P(a)$ for some $a \in D$ | Existential instantiation |
| $P(a)$ for some $a \in D$<br>$\therefore \exists x \in D\ P(x)$ | Existential generalization |

## 4.1.4. Proving Universal Statements by Exhaustion

Given an universal conditional statement:

$$\forall x \in D, P(x) \rightarrow Q(x).$$

When $D$ is finite or when only a finite number of elements satisfy $P(x)$, we may prove the statement by the method of exhaustion.

Example #3: Prove the following statement

$\forall n \in \mathbb{Z}$, if $n$ is even and $4 \leq n \leq 26$, then $n$ can be written as a sum of two primes.

Proof (by method of exhaustion):

- 4 = 2 + 2
- 6 = 3 + 3
- 8 = 3 + 5
- 10 = 5 + 5
- 12 = 5 + 7
- 14 = 11 + 3
- 16 = 5 + 11
- 18 = 7 + 11
- 20 = 7 + 13
- 22 = 5 + 17
- 24 = 5 + 19
- 26 = 7 + 19

## 4.1.5. Proving Universal Statements by Generalizing from the Generic Particular

The most powerful technique for proving a universal statement s one that works regardless of the size of the domain (possibly infinite) over which the statement is quantified.

**Generalizing from the Generic Particular**

To show that every element of a set satisfies a certain property, suppose $x$ is a *particular* but *arbitrarily chosen* element of the set, and show that $x$ satisfies the property.

Example #4: Prove that the sum of any two even integers is even.

Proof:

1. Let $m$ and $n$ be two particular but arbitrarily chosen even integers.
   - 1.1 Then $m = 2r$ and $n = 2s$ for some integers $r$ and $s$ (by definition of even number)
   - 1.2 $m + n = 2r + 2s = 2(r + s)$ (by basic algebra)
   - 1.3 $2(r + s)$ is an integer (by closure under integer addition and multiplication) and an even number (by definition of even number)
   - 1.4 Hence $m + n$ is an even number.
2. Therefore the sum of any two even integers is even.

**Definition: Rational Numbers**

A real number $r$ is rational if, and only if, it can be expressed as a quotient of two integers with a nonzero denominator.

A real number that is not rational is irrational.

$r$ is rational $\Leftrightarrow \exists$ integers $a$ and $b$ such that $r = \frac{a}{b}$ and $b \neq 0$.

## 4.1.2. Proving Existential Statements by Constructive Proof

An existential statement:

$$\exists x \in D \text{ s.t. } Q(x)$$

is true iff $Q(x)$ is true for at least one $x$ in $D$.

To prove such statement, we may use constructive proofs of existence:

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

Example #1

a. Prove that there exists an even integer $n$ that can be written in two ways as a sum of two prime numbers.

b. Suppose $r$ and $s$ are integers. Prove that there is an integer $k$ such that $22r + 18s = 2k$.

a. Let $n = 10$. Then 10 = 5 + 5 = 3 + 7, where 3, 5 and 7 are all prime numbers.

Note that the question does not say that the two prime numbers must be distinct.

b. Let $k = 11r + 9s$. Then $k$ is an integer because it is a sum of products of integers (by closure property); and $2k = 2(11r + 9s) = 22r + 18s$ (by distributive law).

## 4.1.3. Disproving Universal Statements by Counterexample

Given an universal (conditional) statement:

$$\forall x \in D, P(x) \rightarrow Q(x).$$

Showing this statement is false is equivalent to showing that its negation is true.

The negation of the above statement is an existential statement:

$$\exists x \in D, P(x) \wedge \sim Q(x).$$

To prove that an existential statement is true, we use an example (constructive proof), which is called the counterexample for the original universal conditional statement.

**Disproof by Counterexample**

To disprove a statement of the form

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

Find a value of $x$ in $D$ for which the hypothesis $P(x)$ is true but the conclusion $Q(x)$ is false.

Such an $x$ is called a counterexample.

Example #2: Disprove the following statement

$$\forall a, b \in \mathbb{R}, \text{ if } a^2 = b^2 \text{ then } a = b.$$

Counterexample: Let $a = 1$ and $b = -1$. Then $a^2 = 1^2 = 1$ and $b^2 = (-1)^2 = 1$ and so $a^2 = b^2$. But $a \neq b$.

**Corollary**

A result that is a simple deduction from a theorem.

Example:

- (Chapter 4)
  Theorem 4.2.2 (5th: 4.3.2) The sum of any two rational numbers is rational
  Corollary 4.2.3 (5th: 4.3.3) The double of a rational number is rational.

**Theorem 4.3.3 (5th: 4.4.3) Transitivity of Divisibility**

For all integers $a$, $b$ and $c$, if $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof:

1. Suppose $a, b, c$ are integers s.t. $a \mid b$ and $b \mid c$.
   - 1.1 Then $b = ar$ and $c = bs$ for some integers $r$ and $s$. (by definition of divisibility)
   - 1.2 Then $c = bs = (ar)s$ (by substitution) $= a(rs)$ (associativity)
   - 1.3 Let $k = rs$, then $k$ is an integer (by closure property) and $c = ak$.
2. Therefore $a \mid c$.

## 4.4.1. Indirect Proof: Proof by Contradiction

Sometimes when a direct proof is hard to derive, we can try indirect proof.

Example: Theorem 4.7.1 (5th: 4.8.1) $\sqrt{2}$ is irrational.

**Proof by Contradiction**

1. Suppose the statement to be proved, $S$, is false. That is, the negation of the statement, $\sim S$, is true.
2. Show that this supposition leads logically to a contradiction.
3. Conclude that the statement $S$ is true.

**Theorem 4.6.1 (5th: 4.7.1)**

There is no greatest integer.

Proof (by contradiction):

1. Suppose not, i.e. there is a greatest integer.
   - 1.1 Let call this greatest integer $g$, and $g \geq n$ for all integers $n$.
   - 1.2 Let $G = g + 1$.
   - 1.3 Now, $G$ is an integer (closure of integers under addition) and $G > g$.
   - 1.4 Hence, $g$ is not the greatest integer → contradicting 1.1.
2. Hence, the supposition that there is a greatest integer is false.
3. Therefore, there is no greatest integer.

**Proof by Contraposition**

1. Statement to be proved: $\forall x \in D, P(x) \rightarrow Q(x)$.
2. Rewrite the statement into its contrapositive form:
   $\forall x \in D, \sim Q(x) \rightarrow \sim P(x)$.
3. Prove the contrapositive statement by a direct proof.
   - 3.1 Suppose $x$ is an (particular but arbitrarily chosen) element of $D$ s.t. $Q(x)$ is false.
   - 3.2 Show that $P(x)$ is false.
4. Therefore, the original statement $\forall x \in D, P(x) \rightarrow Q(x)$ is true.

**Proposition 4.6.4 (5th: 4.7.4)**

For all integers $n$, if $n^2$ is even than $n$ is even.

Proof (by contraposition):

1. Contrapositive statement:
   For all integers $n$, if $n$ is odd then $n^2$ is odd.
2. Let $n$ be an arbitrarily chosen odd number.
   - 2.1 Then $n = 2k + 1$ for some integer $k$ (definition of odd number).
   - 2.2 Then $n^2 = (2k + 1)(2k + 1) = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$
   - 2.3 Let $m = 2k^2 + 2k$. Now, $m$ is an integer (closure property) and $n^2 = 2m + 1$.
   - 2.4 So $n^2$ is odd.
3. Therefore, for all integers $n$, if $n^2$ is even than $n$ is even.

**Theorem 4.2.1 (5th: 4.3.1)**

Every integer is a rational number.

Proof:

1. Let $a$ be a particular but arbitrarily chosen integer.
   - 1.1 Then $a = \frac{a}{1}$ which is in the form $\frac{a}{b}$ where $a$ and $b(= 1)$ are integers.
   - 1.2 Hence $a$ is a rational number.
2. Therefore every integer is a rational number.

**Theorem 4.2.2 (5th: 4.3.2)**

The sum of any two rational numbers is rational.

Proof:

1. Let $r$ and $s$ be two particular but arbitrarily chosen rational numbers.
   - 1.1 Then $r = \frac{a}{b}$ and $s = \frac{c}{d}$ for some integers $a, b, c, d$ with $b \neq 0$ and $d \neq 0$ (by definition of rational number).
   - 1.2 Then $r + s = \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ (by basic algebra).
   - 1.3 Since $ad + bc$ and $bd$ are integers (by closure under integer addition and multiplication) and $bd \neq 0$, so $r + s$ is rational.
2. Therefore the sum of any two rational numbers is rational.

**Theorem 4.2.2 (5th: 4.3.2)**

The sum of any two rational numbers is rational.

**Corollary 4.2.3 (5th: 4.2.3)**

The double of a rational number is rational.



**Definition: Divisibility**

If $n$ and $d$ are integers and $d \neq 0$, then

$n$ is divisible by $d$ iff $n$ equals $d$ times some integer.

We use the notation $d \mid n$ to mean "$d$ divides $n$". Symbolically, if $n, d \in \mathbb{Z}$ and $d \neq 0$:

$d \mid n \Leftrightarrow \exists k \in \mathbb{Z}$ such that $n = dk$.

**Theorem 4.3.1 (5th: 4.4.1) A Positive Divisor of a Positive Integer**

For all positive integers $a$ and $b$, if $a \mid b$, then $a \leq b$.

Proof (direct proof):

1. Let $a$ and $b$ be two positive integers and $a \mid b$.
   - 1.1 Then there exists an integer $k$ such that $b = ak$ (by definition of divisibility).
   - 1.2 Since both $a$ and $b$ are positive integers, $k$ is positive, i.e. $k \geq 1$.
   - 1.3 Therefore $a \leq ak = b$.
2. Therefore for all positive integers $a$ and $b$, if $a \mid b$, then $a \leq b$.

**Theorem 4.3.2 (5th: 4.4.2) Divisors of 1**

The only divisors of 1 are 1 and -1.

Proof (by division into cases):

1. Suppose $m$ is any integer that divides 1.
   - 1.1 Then there exists an integer $k$ such that $1 = mk$ (by definition of divisibility).
   - 1.2 Since $mk$ is positive, either both $m$ and $k$ are positive, or both negative.
   - 1.3 Case 1: Both $m$ and $k$ are positive.
     - 1.3.1 Since $m \mid 1$, $m \leq 1$ (by Theorem 4.3.1).
     - 1.3.2 Then $m = 1$.
   - 1.4 Case 2: Both $m$ and $k$ are negative.
     - 1.4.1 Then $-m$ is a positive integer divisor of 1, i.e. $-m \mid 1$.
     - 1.4.2 By the same reasoning in 1.3.1 and 1.3.2, $-m = 1$, or $m = -1$.
2. Therefore the only divisors of 1 are 1 and -1.

**Definition**

An integer $n$ is **prime** if, and only if, $n > 1$ and for all positive integers $r$ and $s$, if $n = rs$, then either $r$ or $s$ equals $n$. An integer $n$ is **composite** if, and only if, $n > 1$ and $n = rs$ for some integers $r$ and $s$ with $1 < r < n$ and $1 < s < n$.

In symbols: For each integer $n$ with $n > 1$,

$$n \text{ is prime} \iff \forall \text{ positive integers } r \text{ and } s, \text{ if } n = rs \text{ then either } r = 1 \text{ and } s = n \text{ or } r = n \text{ and } s = 1.$$

$$n \text{ is composite} \iff \exists \text{ positive integers } r \text{ and } s \text{ such that } n = rs \text{ and } 1 < r < n \text{ and } 1 < s < n.$$

**Theorem 4.1.1**

The sum of any two even integers is even.

**Proof:** Suppose $m$ and $n$ are any *[particular but arbitrarily chosen]* even integers. *[We must show that $m + n$ is even.]* By definition of even, $m = 2r$ and $n = 2s$ for some integers $r$ and $s$. Then

$$\begin{aligned} m + n &= 2r + 2s && \text{by substitution} \\ &= 2(r + s) && \text{by factoring out a 2.} \end{aligned}$$

Let $t = r + s$. Note that $t$ is an integer because it is a sum of integers. Hence

$$m + n = 2t \quad \text{where } t \text{ is an integer.}$$

It follows by definition of even that $m + n$ is even. *[This is what we needed to show.]*†

**Theorem 4.2.1**

The difference of any odd integer and any even integer is odd.

**Proof:**

1. Suppose $a$ is any odd integer and $b$ is any even integer. *[We must show that $a - b$ is odd.]*
2. By definition of odd, $a = 2r + 1$ for some integer $r$, and $b = 2s$ for some integer $s$.
3. Then $a - b = (2r + 1) - 2s$ by substitution
4. $= 2r - 2s + 1$ by combining like terms
5. $= 2(r - s) + 1$ by factoring out 2.
6. Let $t = r - s$.
7. Then $t$ is an integer because it is a difference of integers.
8. So, by substitution, $a - b = 2t + 1$, where $t$ is an integer.
9. Hence $a - b$ is odd *[as was to be shown]*.

**Theorem 4.4.5 Unique Factorization of Integers Theorem (Fundamental Theorem of Arithmetic)**

Given any integer $n > 1$, there exist a positive integer $k$, distinct prime numbers $p_1, p_2, \ldots, p_k$, and positive integers $e_1, e_2, \ldots, e_k$ such that

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots p_k^{e_k},$$

and any other expression for $n$ as a product of prime numbers is identical to this except, perhaps, for the order in which the factors are written.

**Definition**

Given any integer $n > 1$, the **standard factored form** of $n$ is an expression of the form

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k},$$

where $k$ is a positive integer, $p_1, p_2, \ldots, p_k$ are prime numbers, $e_1, e_2, \ldots, e_k$ are positive integers, and $p_1 < p_2 < \cdots < p_k$.

**Theorem 4.5.1 The Quotient-Remainder Theorem**

Given any integer $n$ and positive integer $d$, there exist unique integers $q$ and $r$ such that

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

**Theorem 4.5.2 The Parity Property**

Any two consecutive integers have opposite parity.

**Proof:**

Suppose that two *[particular but arbitrarily chosen]* consecutive integers are given; call them $m$ and $m + 1$. *[We must show that one of $m$ and $m + 1$ is even and that the other is odd.]* By the parity property, either $m$ is even or $m$ is odd. *[We break the proof into two cases depending on whether $m$ is even or odd.]*

***Case 1 ($m$ is even):*** In this case, $m = 2k$ for some integer $k$, and so $m + 1 = 2k + 1$, which is odd *[by definition of odd]*. Hence in this case, one of $m$ and $m + 1$ is even and the other is odd.

***Case 2 ($m$ is odd):*** In this case, $m = 2k + 1$ for some integer $k$, and so $m + 1 = (2k + 1) + 1 = 2k + 2 = 2(k + 1)$. But $k + 1$ is an integer because it is a sum of two integers. Therefore, $m + 1$ equals twice some integer, and thus $m + 1$ is even. Hence in this case also, one of $m$ and $m + 1$ is even and the other is odd.

It follows that regardless of which case actually occurs for the particular $m$ and $m + 1$ that are chosen, one of $m$ and $m + 1$ is even and the other is odd. *[This is what was to be shown.]*

**Theorem 4.4.4 Divisibility by a Prime**

Any integer $n > 1$ is divisible by a prime number.

**Proof:** Suppose $n$ is a *[particular but arbitrarily chosen]* integer that is greater than 1. *[We must show that there is a prime number that divides $n$.]* If $n$ is prime, then $n$ is divisible by a prime number (namely itself), and we are done. If $n$ is not prime, then, as discussed in Example 4.1.2b,

$$n = r_0 s_0 \quad \text{where } r_0 \text{ and } s_0 \text{ are integers and } 1 < r_0 < n \text{ and } 1 < s_0 < n.$$

It follows by definition of divisibility that $r_0 | n$.

If $r_0$ is prime, then $r_0$ is a prime number that divides $n$, and we are done. If $r_0$ is not prime, then

$$r_0 = r_1 s_1 \quad \text{where } r_1 \text{ and } s_1 \text{ are integers and } 1 < r_1 < r_0 \text{ and } 1 < s_1 < r_0.$$

It follows by the definition of divisibility that $r_1 | r_0$. But we already know that $r_0 | n$. Consequently, by transitivity of divisibility, $r_1 | n$.

If $r_1$ is prime, then $r_1$ is a prime number that divides $n$, and we are done. If $r_1$ is not prime, then

$$r_1 = r_2 s_2 \quad \text{where } r_2 \text{ and } s_2 \text{ are integers and } 1 < r_2 < r_1 \text{ and } 1 < s_2 < r_1.$$

It follows by definition of divisibility that $r_2 | r_1$. But we already know that $r_1 | n$. Consequently, by transitivity of divisibility, $r_2 | n$.

If $r_2$ is prime, then $r_2$ is a prime number that divides $n$, and we are done. If $r_2$ is not prime, then we may repeat the previous process by factoring $r_2$ as $r_3 s_3$.

We may continue in this way, factoring successive factors of $n$ until we find a prime factor. We must succeed in a finite number of steps because each new factor is both less than the previous one (which is less than $n$) and greater than 1, and there are fewer than $n$ integers strictly between 1 and $n$.* Thus we obtain a sequence

$$r_0, r_1, r_2, \ldots, r_k,$$

where $k \ge 0$, $1 < r_k < r_{k-1} < \cdots < r_2 < r_1 < r_0 < n$, and $r_i | n$ for each $i = 0, 1, 2, \ldots, k$. The condition for termination is that $r_k$ should be prime. Hence $r_k$ is a prime number that divides $n$. *[This is what we were to show.]*

**Theorem 4.4.1 A Positive Divisor of a Positive Integer**

For all integers $a$ and $b$, if $a$ and $b$ are positive and $a$ divides $b$ then $a \le b$.

**Proof:** Suppose $a$ and $b$ are any positive integers such that $a$ divides $b$. *[We must show that $a \le b$.]* By definition of divisibility, there exists an integer $k$ so that $b = ak$. By property T25 of Appendix A, $k$ must be positive because both $a$ and $b$ are positive. It follows that

$$1 \le k$$

because every positive integer is greater than or equal to 1. Multiplying both sides by $a$ gives

$$a \le ka = b$$

because multiplying both sides of an inequality by a positive number preserves the inequality by property T20 of Appendix A. Thus $a \le b$ *[as was to be shown]*.

**Definition**

Given an integer $n$ and a positive integer $d$,

$$n \textbf{ div } d = \text{the integer quotient obtained when } n \text{ is divided by } d, \text{ and}$$

$$n \textbf{ mod } d = \text{the nonnegative integer remainder obtained when } n \text{ is divided by } d.$$

Symbolically, if $n$ and $d$ are integers and $d > 0$, then

$$n \text{ div } d = q \quad \text{and} \quad n \text{ mod } d = r \iff n = dq + r,$$

where $q$ and $r$ are integers and $0 \le r < d$.

**Definition**

For any real number $x$, the **absolute value of $x$**, denoted $|x|$, is defined as follows:

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

**Theorem 4.5.3**

The square of any odd integer has the form $8m + 1$ for some integer $m$.

**Proof:** Suppose $n$ is a *[particular but arbitrarily chosen]* odd integer. By the quotient-remainder theorem with the divisor equal to 4, $n$ can be written in one of the forms

$$4q \quad \text{or} \quad 4q+1 \quad \text{or} \quad 4q+2 \quad \text{or} \quad 4q+3$$

for some integer $q$. In fact, since $n$ is odd and $4q$ and $4q+2$ are even, $n$ must have one of the forms

$$4q+1 \quad \text{or} \quad 4q+3.$$

***Case 1 ($n = 4q + 1$ for some integer $q$):*** *[We must find an integer $m$ such that $n^2 = 8m + 1$.]* Since $n = 4q + 1$,

$$\begin{aligned} n^2 &= (4q+1)^2 && \text{by substitution} \\ &= (4q+1)(4q+1) && \text{by definition of square} \\ &= 16q^2 + 8q + 1 \\ &= 8(2q^2 + q) + 1 && \text{by the laws of algebra.} \end{aligned}$$

Let $m = 2q^2 + q$. Then $m$ is an integer since 2 and $q$ are integers and sums and products of integers are integers. Thus, substituting,

$$n^2 = 8m + 1 \quad \text{where } m \text{ is an integer.}$$

***Case 2 ($n = 4q + 3$ for some integer $q$):*** *[We must find an integer $m$ such that $n^2 = 8m + 1$.]* Since $n = 4q + 3$,

$$\begin{aligned} n^2 &= (4q+3)^2 && \text{by substitution} \\ &= (4q+3)(4q+3) && \text{by definition of square} \\ &= 16q^2 + 24q + 9 \\ &= 16q^2 + 24q + (8+1) \\ &= 8(2q^2 + 3q + 1) + 1 && \text{by the laws of algebra.} \end{aligned}$$

*[The motivation for the choice of algebra steps was the desire to write the expression in the form $8 \cdot$(some integer) $+ 1$.]*

Let $m = 2q^2 + 3q + 1$. Then $m$ is an integer since 1, 2, 3, and $q$ are integers and sums and products of integers are integers. Thus, substituting,

$$n^2 = 8m + 1 \quad \text{where } m \text{ is an integer.}$$

Cases 1 and 2 show that given any odd integer, whether of the form $4q + 1$ or $4q + 3$, $n^2 = 8m + 1$ for some integer $m$. *[This is what we needed to show.]*

**Theorem 4.5.6 The Triangle Inequality**

For all real numbers $x$ and $y$, $|x + y| \leq |x| + |y|$.

**Proof:** Suppose $x$ and $y$ are any real numbers.

***Case 1 ($x + y \geq 0$):*** In this case, $|x + y| = x + y$, and so, by Lemma 4.5.4,

$$x \leq |x| \quad \text{and} \quad y \leq |y|.$$

Hence, by Theorem T26 of Appendix A,

$$|x + y| = x + y \leq |x| + |y|.$$

***Case 2 ($x + y < 0$):*** In this case, $|x + y| = -(x + y) = (-x) + (-y)$, and so, by Lemmas 4.5.4 and 4.5.5,

$$-x \leq |-x| = |x| \quad \text{and} \quad -y \leq |-y| = |y|.$$

It follows, by Theorem T26 of Appendix A, that

$$|x + y| = (-x) + (-y) \leq |x| + |y|.$$

Hence in both cases $|x + y| \leq |x| + |y|$ *[as was to be shown].*

**Theorem 4.6.1**

For every real number $x$ and every integer $m$, $\lfloor x + m \rfloor = \lfloor x \rfloor + m$.

**Proof:** Suppose any real number $x$ and any integer $m$ are given. *[We must show that $\lfloor x + m \rfloor = \lfloor x \rfloor + m$.]* Let $n = \lfloor x \rfloor$. By definition of floor, $n$ is an integer and

$$n \leq x < n + 1.$$

Add $m$ to all three parts to obtain

$$n + m \leq x + m < n + m + 1$$

*[since adding a number to both sides of an inequality does not change the direction of the inequality].*

Now $n + m$ is an integer *[since $n$ and $m$ are integers and a sum of integers is an integer]*, and so, by definition of floor, the left-hand side of the equation to be shown is

$$\lfloor x + m \rfloor = n + m.$$

But $n = \lfloor x \rfloor$. Hence, by substitution,

$$n + m = \lfloor x \rfloor + m,$$

which is the right-hand side of the equation to be shown. Thus $\lfloor x + m \rfloor = \lfloor x \rfloor + m$ *[as was to be shown].*

**Lemma 4.5.4**

For every real number $r$, $-|r| \leq r \leq |r|$.

**Proof:** Suppose $r$ is any real number. We divide into cases according to whether $r = 0$, $r > 0$, or $r < 0$.

***Case 1 ($r = 0$):*** In this case, by definition of absolute value, $|r| = r = 0$. Since $0 = -0$, we have that $-0 = -|r| = 0 = r = |r|$, and so it is true that

$$-|r| \leq r \leq |r|.$$

***Case 2 ($r > 0$):*** In this case, by definition of absolute value, $|r| = r$. Also, since $r$ is positive and $-|r|$ is negative, $-|r| < r$. Thus it is true that

$$-|r| \leq r \leq |r|.$$

***Case 3 ($r < 0$):*** In this case, by definition of absolute value, $|r| = -r$. Multiplying both sides by $-1$ gives that $-|r| = r$. Also, since $r$ is negative and $|r|$ is positive, $r < |r|$. Thus it is also true in this case that

$$-|r| \leq r \leq |r|.$$

Hence, in every case,

$$-|r| \leq r \leq |r|$$

*[as was to be shown].*

**Lemma 4.5.5**

For every real number $r$, $|-r| = |r|$.

**Proof:** Suppose $r$ is any real number. By Theorem T23 in Appendix A, if $r > 0$, then $-r < 0$, and if $r < 0$, then $-r > 0$. Thus

$$\begin{aligned} |-r| &= \begin{cases} -r & \text{if } -r > 0 \\ 0 & \text{if } -r = 0 \\ -(-r) & \text{if } -r < 0 \end{cases} && \text{by definition of absolute value} \\ &= \begin{cases} -r & \text{if } -r > 0 \\ 0 & \text{if } r = 0 \\ r & \text{if } -r < 0 \end{cases} && \text{because } -(-r) = r \text{ by Theorem T4 in Appendix A, and when } -r = 0, \text{ then } r = 0 \\ &= \begin{cases} -r & \text{if } r < 0 \\ 0 & \text{if } r = 0 \\ r & \text{if } r > 0 \end{cases} && \text{because, by Theorem T24 in Appendix A, when } -r > 0, \text{ then } r < 0, \text{ when } -r < 0, \text{ then } r > 0 \\ &= \begin{cases} r & \text{if } r \geq 0 \\ -r & \text{if } r < 0 \end{cases} && \text{by reformatting the previous result} \\ &= |r| && \text{by definition of absolute value.} \end{aligned}$$

**Definition**

Given any real number $x$, the **floor of $x$**, denoted $\lfloor x \rfloor$, is defined as follows:

$$\lfloor x \rfloor = \text{that unique integer } n \text{ such that } n \leq x < n + 1.$$

Symbolically, if $x$ is a real number and $n$ is an integer, then

$$\lfloor x \rfloor = n \quad \Leftrightarrow \quad n \leq x < n + 1.$$

**Definition**

Given any real number $x$, the **ceiling of $x$**, denoted $\lceil x \rceil$, is defined as follows:

$$\lceil x \rceil = \text{that unique integer } n \text{ such that } n - 1 < x \leq n.$$

Symbolically, if $x$ is a real number and $n$ is an integer, then

$$\lceil x \rceil = n \quad \Leftrightarrow \quad n - 1 < x \leq n.$$

**Theorem 4.6.2 The Floor of $n/2$**

For any integer $n$,

$$\left\lfloor \frac{n}{2} \right\rfloor = \begin{cases} \dfrac{n}{2} & \text{if } n \text{ is even} \\ \dfrac{n-1}{2} & \text{if } n \text{ is odd.} \end{cases}$$

**Proof:** Suppose $n$ is a *[particular but arbitrarily chosen]* integer. By the quotient-remainder theorem, either $n$ is odd or $n$ is even.

***Case 1 (n is odd):*** In this case, $n = 2k + 1$ for some integer $k$. *[We must show that* $\lfloor n/2 \rfloor = (n-1)/2$*.]* But the left-hand side of the equation to be shown is

$$\left\lfloor \frac{n}{2} \right\rfloor = \left\lfloor \frac{2k+1}{2} \right\rfloor = \left\lfloor \frac{2k}{2} + \frac{1}{2} \right\rfloor = \left\lfloor k + \frac{1}{2} \right\rfloor = k$$

because $k$ is an integer and $k \le k + 1/2 < k + 1$. And the right-hand side of the equation to be shown is

$$\frac{n-1}{2} = \frac{(2k+1)-1}{2} = \frac{2k}{2} = k$$

also. So since both the left-hand and right-hand sides equal $k$, they are equal to each other. That is, $\lfloor \frac{n}{2} \rfloor = \frac{n-1}{2}$ *[as was to be shown].*

***Case 2 (n is even):*** In this case, $n = 2k$ for some integer $k$. *[We must show that* $\lfloor n/2 \rfloor = n/2$*.]* The rest of the proof of this case is left as an exercise.

**Theorem 4.7.3**

The sum of any rational number and any irrational number is irrational.

**Proof:**

*[We take the negation of the theorem and suppose it to be true.]* Suppose not. That is, suppose there is a rational number $r$ and an irrational number $s$ such that $r + s$ is rational. *[We must deduce a contradiction.]* By definition of rational, $r = a/b$ and $r + s = c/d$ for some integers $a$, $b$, $c$, and $d$ with $b \ne 0$ and $d \ne 0$. By substitution,

$$\frac{a}{b} + s = \frac{c}{d},$$

and so

$$s = \frac{c}{d} - \frac{a}{b} \qquad \text{by subtracting } a/b \text{ from both sides}$$
$$= \frac{bc - ad}{bd} \qquad \text{by the laws of algebra.}$$

Now $bc - ad$ and $bd$ are both integers *[since a, b, c, and d are integers and since products and differences of integers are integers]*, and $bd \ne 0$ *[by the zero product property]*. Hence $s$ is a quotient of the two integers $bc - ad$ and $bd$ with $bd \ne 0$. Thus, by definition of rational, $s$ is rational, which contradicts the supposition that $s$ is irrational. *[Hence the supposition is false and the theorem is true.]*

**Theorem 4.8.1 Irrationality of $\sqrt{2}$**

$\sqrt{2}$ is irrational.

**Proof (by contradiction):** *[We take the negation and suppose it to be true.]* Suppose not. That is, suppose $\sqrt{2}$ is rational. Then there are integers $m$ and $n$ with no common factors such that

$$\sqrt{2} = \frac{m}{n} \qquad 4.8.1$$

*[by dividing m and n by any common factors if necessary]. [We must derive a contradiction.]* Squaring both sides of equation (4.8.1) gives

$$2 = \frac{m^2}{n^2}.$$

Or, equivalently,

$$m^2 = 2n^2. \qquad 4.8.2$$

Note that equation (4.8.2) implies that $m^2$ is even (by definition of even). It follows that $m$ is even (by Proposition 4.7.4). We file this fact away for future reference and also deduce (by definition of even) that

$$m = 2k \quad \text{for some integer } k. \qquad 4.8.3$$

Substituting equation (4.8.3) into equation (4.8.2), we see that

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

Dividing both sides of the right-most equation by 2 gives

$$n^2 = 2k^2.$$

Consequently, $n^2$ is even, and so $n$ is even (by Proposition 4.7.4). But we also know that $m$ is even. *[This is the fact we filed away.]* Hence both $m$ and $n$ have a common factor of 2. But this contradicts the supposition that $m$ and $n$ have no common factors. *[Hence the supposition is false and so the theorem is true.]*

**Theorem 4.6.3**

If $n$ is any integer and $d$ is a positive integer, and if $q = \lfloor n/d \rfloor$ and $r = n - d \cdot \lfloor n/d \rfloor$, then

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

**Proof:** Suppose $n$ is any integer, $d$ is a positive integer, $q = \lfloor n/d \rfloor$, and $r = n - d \cdot \lfloor n/d \rfloor$. *[We must show that* $n = dq + r$ *and* $0 \le r < d$*.]* By substitution,

$$dq + r = d \cdot \left\lfloor \frac{n}{d} \right\rfloor + \left( n - d \cdot \left\lfloor \frac{n}{d} \right\rfloor \right) = n.$$

So it remains only to show that $0 \le r < d$. But $q = \lfloor n/d \rfloor$. Thus, by definition of floor,

$$q \le \frac{n}{d} < q + 1.$$

Then

$$dq \le n < dq + d \qquad \text{by multiplying all parts by } d$$

and so

$$0 \le n - dq < d \qquad \text{by subtracting } dq \text{ from all parts.}$$

But

$$r = n - d\left\lfloor \frac{n}{d} \right\rfloor = n - dq.$$

Hence

$$0 \le r < d \qquad \text{by substitution.}$$

*[This is what was to be shown.]*

**Theorem 4.7.2**

There is no integer that is both even and odd.

**Proof:** *[We take the negation of the theorem and suppose it to be true.]* Suppose not. That is, suppose there is at least one integer $n$ that is both even and odd.

*[We must deduce a contradiction.]* By definition of even, $n = 2a$ for some integer $a$, and by definition of odd, $n = 2b + 1$ for some integer $b$. Consequently,

$$2a = 2b + 1 \qquad \text{by equating the two expressions for } n,$$

and so

$$\begin{aligned} 2a - 2b &= 1 \\ 2(a - b) &= 1 \\ a - b &= 1/2 \qquad \text{by algebra.} \end{aligned}$$

Now since $a$ and $b$ are integers, the difference $a - b$ must also be an integer. But $a - b = 1/2$, and $1/2$ is not an integer. Thus $a - b$ is an integer and $a - b$ is not an integer, which is a contradiction. *[This contradiction shows that the supposition is false and, hence, that the theorem is true.]*

**Proposition 4.8.2**

$1 + 3\sqrt{2}$ is irrational.

**Proof:** Suppose not. Suppose $1 + 3\sqrt{2}$ is rational. *[We must derive a contradiction.]* Then by definition of rational,

$$1 + 3\sqrt{2} = \frac{a}{b} \quad \text{for some integers } a \text{ and } b \text{ with } b \ne 0.$$

It follows that

$$3\sqrt{2} = \frac{a}{b} - 1 \qquad \text{by subtracting 1 from both sides}$$
$$= \frac{a}{b} - \frac{b}{b} \qquad \text{by substitution}$$
$$= \frac{a-b}{b} \qquad \text{by the rule for subtracting fractions with a common denominator.}$$

Hence

$$\sqrt{2} = \frac{a-b}{3b} \qquad \text{by dividing both sides by 3.}$$

But $a - b$ and $3b$ are integers (since $a$ and $b$ are integers and differences and products of integers are integers), and $3b \ne 0$ by the zero product property. Hence $\sqrt{2}$ is a quotient of the two integers $a - b$ and $3b$ with $3b \ne 0$, and so $\sqrt{2}$ is rational (by definition of rational). This contradicts the fact that $\sqrt{2}$ is irrational. *[The contradiction shows that the supposition is false.]* Hence $1 + 3\sqrt{2}$ is irrational.

**Proposition 4.8.3**

For any integer $a$ and any prime number $p$, if $p|a$ then $p \nmid (a+1)$.

**Proof (by contradiction):** Suppose not. That is, suppose there exist an integer $a$ and a prime number $p$ such that $p|a$ and $p|(a+1)$. Then, by definition of divisibility, there exist integers $r$ and $s$ such that $a = pr$ and $a+1 = ps$. It follows that

$$1 = (a+1) - a = ps - pr = p(s-r),$$

and so (since $s-r$ is an integer) $p|1$. But, by Theorem 4.4.2, the only integer divisors of 1 are 1 and $-1$, and $p > 1$ because $p$ is prime. Thus $p \leq 1$ and $p > 1$, which is a contradiction. *[Hence the supposition is false, and the proposition is true.]*

**Theorem 4.8.4 Infinitude of the Primes**

The set of prime numbers is infinite.

**Proof (by contradiction):** Suppose not. That is, suppose the set of prime numbers is finite. *[We must deduce a contradiction.]* Then some prime number $p$ is the largest of all the prime numbers, and hence we can list the prime numbers in ascending order:

$$2, 3, 5, 7, 11, \ldots, p.$$

Let $N$ be the product of all the prime numbers plus 1:

$$N = (2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p) + 1$$

Then $N > 1$, and so, by Theorem 4.4.4, $N$ is divisible by some prime number $q$. Because $q$ is prime, $q$ must equal one of the prime numbers $2, 3, 5, 7, 11, \ldots, p$. Thus, by definition of divisibility, $q$ divides $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p$, and so, by Proposition 4.8.3, $q$ does not divide $(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p) + 1$, which equals $N$. Hence $N$ is divisible by $q$ and $N$ is not divisible by $q$, and we have reached a contradiction. *[Therefore, the supposition is false and the theorem is true.]*

**Definition**

Let $a$ and $b$ be integers that are not both zero. The **greatest common divisor** of $a$ and $b$, denoted $\mathbf{gcd}(a, b)$, is that integer $d$ with the following properties:

1. $d$ is a common divisor of both $a$ and $b$. In other words,
$$d|a \quad \text{and} \quad d|b.$$
2. For every integer $c$, if $c$ is a common divisor of both $a$ and $b$, then $c$ is less than or equal to $d$. In other words,
$$\text{for every integer } c, \text{ if } c|a \text{ and } c|b \text{ then } c \leq d.$$

**Lemma 4.10.1**

If $r$ is a positive integer, then $\gcd(r, 0) = r$.

**Proof:** Suppose $r$ is a positive integer. *[We must show that the greatest common divisor of both $r$ and 0 is $r$.]* Certainly, $r$ is a common divisor of both $r$ and 0 because $r$ divides itself and also $r$ divides 0 (since every positive integer divides 0). Also no integer larger than $r$ can be a common divisor of $r$ and 0 (since no integer larger than $r$ can divide $r$). Hence $r$ is the greatest common divisor of $r$ and 0.

**Lemma 4.10.2**

If $a$ and $b$ are any integers not both zero, and if $q$ and $r$ are any integers such that

$$a = bq + r,$$

then

$$\gcd(a, b) = \gcd(b, r).$$

**Proof:** *[The proof is divided into two sections: (1) proof that $\gcd(a, b) \leq \gcd(b, r)$, and (2) proof that $\gcd(b, r) \leq \gcd(a, b)$. Since each gcd is less than or equal to the other, the two must be equal.]*

1. **gcd(a, b) ≤ gcd(b, r):**
   a. *[We will first show that any common divisor of a and b is also a common divisor of b and r.]*
   Let $a$ and $b$ be integers, not both zero, and let $c$ be a common divisor of $a$ and $b$. Then $c|a$ and $c|b$, and so, by definition of divisibility, $a = nc$ and $b = mc$, for some integers $n$ and $m$. Substitute into the equation
   $$a = bq + r$$
   to obtain
   $$nc = (mc)q + r.$$
   Then solve for $r$:
   $$r = nc - (mc)q = (n - mq)c.$$
   Now $n - mq$ is an integer, and so, by definition of divisibility, $c|r$. Because we already know that $c|b$, we can conclude that $c$ is a common divisor of $b$ and $r$ *[as was to be shown]*.
   b. *[Next we show that $\gcd(a, b) \leq \gcd(b, r)$.]*
   Now the greatest common divisor of $a$ and $b$ is defined because $a$ and $b$ are not both zero. Also, by part (a), every common divisor of $a$ and $b$ is a common divisor of $b$ and $r$, and so the greatest common divisor of $a$ and $b$ is a common divisor of $b$ and $r$. But then $\gcd(a, b)$ (being one of the common divisors of $b$ and $r$) is less than or equal to the greatest common divisor of $b$ and $r$:
   $$\gcd(a, b) \leq \gcd(b, r).$$
2. **gcd(b, r) ≤ gcd(a, b):**
   The second part of the proof is very similar to the first part. It is left as an exercise.

**Definition 5.1.1.** (1) A *set* is an unordered collection of objects.

(2) These objects are called the *members* or *elements* of the set.

(3) Write

| | | | |
|---|---|---|---|
| $x \in A$ | for | $x$ is an element of $A$; | |
| $x \notin A$ | for | $x$ is not an element of $A$; | |
| $x, y \in A$ | for | $x, y$ are elements of $A$; | |
| $x, y \notin A$ | for | $x, y$ are not elements of $A$; | etc. |

(4) We may read $x \in A$ also as "$x$ is in $A$" or "$A$ *contains* $x$ (as an element)".

| Symbol | Meaning | Examples | Non-examples |
|---|---|---|---|
| $\mathbb{N}$ | the set of all natural numbers | $0, 1, 2, 3, 31 \in \mathbb{N}$ | $-1, \frac{1}{2} \notin \mathbb{N}$ |
| $\mathbb{Z}$ | the set of all integers | $0, 1, -1, 2, -10 \in \mathbb{Z}$ | $\frac{1}{2}, \sqrt{2} \notin \mathbb{Z}$ |
| $\mathbb{Q}$ | the set of all rational numbers | $-1, 10, \frac{1}{2}, -\frac{7}{5} \in \mathbb{Q}$ | $\sqrt{2}, \pi, \sqrt{-1} \notin \mathbb{Q}$ |
| $\mathbb{R}$ | the set of all real numbers | $-1, 10, -\frac{3}{2}, \sqrt{2}, \pi \in \mathbb{R}$ | $\sqrt{-1}, \sqrt{-10} \notin \mathbb{R}$ |
| $\mathbb{C}$ | the set of all complex numbers | $-1, 10, -\frac{3}{2}, \sqrt{2}, \pi, \sqrt{-1}, \sqrt{-10} \in \mathbb{C}$ | |
| $\mathbb{Z}^+$ | the set of all positive integers | $1, 2, 3, 31 \in \mathbb{Z}^+$ | $0, -1, -12 \notin \mathbb{Z}^+$ |
| $\mathbb{Z}^-$ | the set of all negative integers | $-1, -2, -3, -31 \in \mathbb{Z}^-$ | $0, 1, 12 \notin \mathbb{Z}^-$ |
| $\mathbb{Z}_{\geqslant 0}$ | the set of all non-negative integers | $0, 1, 2, 3, 31 \in \mathbb{Z}_{\geqslant 0}$ | $-1, -12 \notin \mathbb{Z}_{\geqslant 0}$ |

$\mathbb{Q}^+$, $\mathbb{Q}^-$, $\mathbb{Q}_{\geqslant m}$, $\mathbb{R}^+$, $\mathbb{R}^-$, $\mathbb{R}_{\geqslant m}$, etc. are defined similarly.

**Note 5.1.3.** Some define $0 \notin \mathbb{N}$, but in this module we do *not*.

**Definition 5.1.4** (roster notation)**.** (1) The set whose only elements are $x_1, x_2, \ldots, x_n$ is denoted $\{x_1, x_2, \ldots, x_n\}$.

(2) The set whose only elements are $x_1, x_2, x_3, \ldots$ is denoted $\{x_1, x_2, x_3, \ldots\}$.

**To check whether an object $z$ is an element of a set $S = \{x_1, x_2, \ldots, x_n\}$.** If $z$ is in the list $x_1, x_2, \ldots, x_n$, then $z \in S$, else $z \notin S$.

**Definition 5.1.6** (set-builder notation)**.** Let $U$ be a set and $P(x)$ be a predicate over $U$. Then the set of all elements $x \in U$ such that $P(x)$ is true is denoted

$$\{x \in U : P(x)\} \quad \text{or} \quad \{x \in U \mid P(x)\}.$$

This is read as "the set of all $x$ in $U$ such that $P(x)$".

**To check whether an object $z$ is an element of $S = \{x \in U : P(x)\}$.** If $z \in U$ and $P(z)$ is true, then $z \in S$, else $z \notin S$. Hence $z \notin U$ implies $z \notin S$, and $P(z)$ is false implies $z \notin S$.

**Definition 5.1.8** (replacement notation)**.** Let $A$ be a set and $t(x)$ be a term in a variable $x$. Then the set of all objects of the form $t(x)$ where $x$ ranges over the elements of $A$ is denoted

$$\{t(x) : x \in A\} \quad \text{or} \quad \{t(x) \mid x \in A\}.$$

This is read as "the set of all $t(x)$ where $x \in A$".

**To check whether an object $z$ is an element of $S = \{t(x) : x \in A\}$.** If there is an element $x \in A$ such that $t(x) = z$, then $z \in S$, else $z \notin S$.

**Definition 5.1.10.** Two sets are *equal* if they have the same elements, i.e., for all sets $A, B$,

$$A = B \quad \Leftrightarrow \quad \forall z \ (z \in A \Leftrightarrow z \in B).$$

**Convention 5.1.11.** In mathematical definitions, people often use "if" between the term being defined and the phrase being used to define the term. This is the *only* situation in mathematics when "if" should be understood as a (special) "if and only if".

## Slogan 5.1.13. Order and repetition do not matter.

**Theorem 5.1.17.** There exists a unique set with no element, i.e.,

- there is a set with no element; and (existence part)
- for all sets $A, B$, if both $A$ and $B$ have no element, then $A = B$. (uniqueness part)

**Definition 5.1.18.** The set with no element is called the *empty set*. It is denoted by $\varnothing$.

**Definition 5.1.19.** Let $A, B$ be sets. Call $A$ a *subset* of $B$, and write $A \subseteq B$, if

$$\forall z\ (z \in A \Rightarrow z \in B).$$

Alternatively, we may say that $B$ *includes* $A$, and write $B \supseteq A$ in this case.

**Remark 5.1.22.** Let $A, B$ be sets.

(1) $$A \not\subseteq B \quad \Leftrightarrow \quad \exists z\ (z \in A \text{ and } z \notin B).$$

(2) $$A = B \quad \Leftrightarrow \quad A \subseteq B \text{ and } B \subseteq A.$$

(3) $$\varnothing \subseteq A \quad \text{and} \quad A \subseteq A.$$

**Definition 5.1.23.** Let $A, B$ be sets. Call $A$ a *proper subset* of $B$, and write $A \subsetneq B$, if $A \subseteq B$ and $A \neq B$. In this case, we may say that the inclusion of $A$ in $B$ is *proper* or *strict*.

**Definition 5.2.1.** Let $A$ be a set. The set of all subsets of $A$, denoted $\mathcal{P}(A)$, is called the *power set* of $A$.

**Definition 5.2.3.** (1) A set is *finite* if it has finitely many (distinct) elements. It is *infinite* if it is not finite.

(2) Let $A$ be a finite set. The *cardinality* of $A$, or the *size* of $A$, is the number of (distinct) elements in $A$. It is denoted by $|A|$.

(3) Sets of size 1 are called *singletons*.

**Theorem 5.2.4.** Let $A$ be a finite set. Then $|\mathcal{P}(A)| = 2^{|A|}$.

**Definition 5.2.6.** An *ordered pair* is an expression of the form

$$(x, y).$$

Let $(x_1, y_1)$ and $(x_2, y_2)$ be ordered pairs. Then

$$(x_1, y_1) = (x_2, y_2) \quad \Leftrightarrow \quad x_1 = x_2 \quad \text{and} \quad y_1 = y_2.$$

**Definition 5.2.8.** Let $A, B$ be sets. The *Cartesian product* of $A$ and $B$, denoted $A \times B$, is defined to be

$$\{(x, y) : x \in A \text{ and } y \in B\}.$$

Read $A \times B$ as "$A$ cross $B$".

**Note 5.2.10.** $|\{a, b\} \times \{1, 2, 3\}| = 6 = 2 \times 3 = |\{a, b\}| \times |\{1, 2, 3\}|$.

**Definition 5.2.11.** Let $n \in \{x \in \mathbb{Z} : x \geqslant 2\}$. An *ordered $n$-tuple* is an expression of the form

$$(x_1, x_2, \ldots, x_n).$$

Let $(x_1, x_2, \ldots, x_n)$ and $(y_1, y_2, \ldots, y_n)$ be ordered $n$-tuples. Then

$$(x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_n) \quad \Leftrightarrow \quad x_1 = y_1 \text{ and } x_2 = y_2 \text{ and } \ldots \text{ and } x_n = y_n.$$

**Definition 5.2.13.** Let $n \in \{x \in \mathbb{Z} : x \geqslant 2\}$ and $A_1, A_2, \ldots, A_n$ be sets. The *Cartesian product* of $A_1, A_2, \ldots, A_n$, denoted $A_1 \times A_2 \times \cdots \times A_n$, is defined to be

$$\{(x_1, x_2, \ldots, x_n) : x_1 \in A_1 \text{ and } x_2 \in A_2 \text{ and } \ldots \text{ and } x_n \in A_n\}.$$

If $A$ is a set, then $A^n = \underbrace{A \times A \times \cdots \times A}_{n\text{-many } A\text{'s}}$.

**Definition 5.3.1.** Let $A, B$ be sets.

(1) The *union* of $A$ and $B$, denoted $A \cup B$, is defined by

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

Read $A \cup B$ as "$A$ union $B$".

(2) The *intersection* of $A$ and $B$, denoted $A \cap B$, is defined by

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

Read $A \cap B$ as "$A$ intersect $B$".

(3) The *complement* of $B$ in $A$, denoted $A - B$ or $A \setminus B$, is defined by

$$A \setminus B = \{x : x \in A \text{ and } x \notin B\}.$$

Read $A \setminus B$ as "$A$ minus $B$".

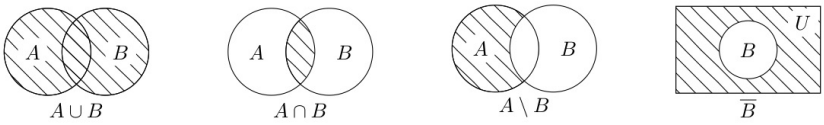



Figure 5.2: Boolean operations on sets

**Convention and terminology 5.3.2.** When working in a particular context, one usually works within a fixed set $U$ which includes all the sets one may talk about, so that one only needs to consider the elements of $U$ when proving set equality and inclusion (because no other object can be the element of a set). This $U$ is called a *universal set*.

**Definition 5.3.3.** Let $B$ be a set. In a context where $U$ is the universal set (so that implicitly $U \supseteq B$), the *complement* of $B$, denoted $\overline{B}$ or $B^c$, is defined by

$$\overline{B} = U \setminus B.$$

**Theorem 5.3.5** (Set Identities)**.** For all set $A, B, C$ in a context where $U$ is the universal set, the following hold.

| | | |
|---|---|---|
| Identity Laws | $A \cup \varnothing = A$ | $A \cap U = A$ |
| Universal Bound Laws | $A \cup U = U$ | $A \cap \varnothing = \varnothing$ |
| Idempotent Laws | $A \cup A = A$ | $A \cap A = A$ |
| Double Complement Law | $\overline{(\overline{A})} = A$ | |
| Commutative Laws | $A \cup B = B \cup A$ | $A \cap B = B \cap A$ |
| Associative Laws | $(A \cup B) \cup C = A \cup (B \cup C)$ | $(A \cap B) \cap C = A \cap (B \cap C)$ |
| Distributive Laws | $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ | $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ |
| De Morgan's Laws | $\overline{A \cup B} = \overline{A} \cap \overline{B}$ | $\overline{A \cap B} = \overline{A} \cup \overline{B}$ |
| Absorption Laws | $A \cup (A \cap B) = A$ | $A \cap (A \cup B) = A$ |
| Complement Laws | $A \cup \overline{A} = U$ | $A \cap \overline{A} = \varnothing$ |
| Set Difference Law | $A \setminus B = A \cap \overline{B}$ | |
| Top and Bottom Laws | $\overline{\varnothing} = U$ | $\overline{U} = \varnothing$ |

**One of De Morgan's Laws.** Work in the universal set $U$. For all sets $A, B$,

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

**Venn Diagrams.** In the left diagram below, hatch the regions representing $A$ and $B$ with ⧹ and ⧸ respectively. In the right diagram below, hatch the regions representing $\overline{A}$ and $\overline{B}$ with ⧹ and ⧸ respectively.


Then the □ region represents $\overline{A \cup B}$ in the left diagram, and the ⧄ region represents $\overline{A} \cap \overline{B}$ in the right diagram. Since these regions occupy the same region in the respective diagrams, we infer that $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

**Note 5.3.6.** This argument depends on the fact that each possibility for membership in $A$ and $B$ is represented by a region in the diagram.

**Proof using a truth table.** The rows in the following table list all the possibilities for an element $x \in U$:

| $x \in A$ | $x \in B$ | $x \in A \cup B$ | $x \in \overline{A \cup B}$ | $x \in \overline{A}$ | $x \in \overline{B}$ | $x \in \overline{A} \cap \overline{B}$ |
|---|---|---|---|---|---|---|
| T | T | T | F | F | F | F |
| T | F | T | F | F | T | F |
| F | T | T | F | T | F | F |
| F | F | F | T | T | T | T |

Since the columns under "$x \in \overline{A \cup B}$" and "$x \in \overline{A} \cap \overline{B}$" are the same, for any $x \in U$,

$$x \in \overline{A \cup B} \quad \Leftrightarrow \quad x \in \overline{A} \cap \overline{B}$$

no matter in which case we are. So $\overline{A \cup B} = \overline{A} \cap \overline{B}$. □

**Direct proof.** 1. Let $z \in U$.

2. 2.1. Then $z \in \overline{A \cup B}$
   2.2. $\Leftrightarrow$ $z \notin A \cup B$ by the definition of $\overline{\cdot}$;
   2.3. $\Leftrightarrow$ $\sim((z \in A) \vee (z \in B))$ by the definition of $\cup$;
   2.4. $\Leftrightarrow$ $(z \notin A) \wedge (z \notin B)$ by De Morgan's Laws for propositions;
   2.5. $\Leftrightarrow$ $(z \in \overline{A}) \wedge (z \in \overline{B})$ by the definition of $\overline{\cdot}$;
   2.6. $\Leftrightarrow$ $z \in \overline{A} \cap \overline{B}$ by the definition of $\cap$. □

**Definition 5.3.10.** (1) Two sets $A, B$ are *disjoint* if $A \cap B = \varnothing$.

(2) Sets $A_1, A_2, \ldots, A_n$ are *pairwise disjoint* or *mutually disjoint* if $A_i \cap A_j = \varnothing$ for all distinct $i, j \in \{1, 2, \ldots, n\}$.

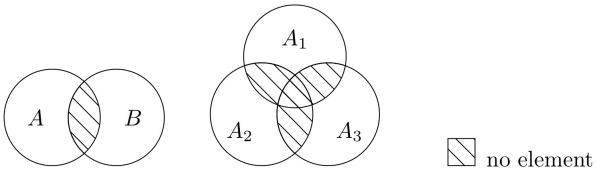



Figure 5.3: (Pairwise) disjoint sets

**Theorem 5.3.12.** (1) Let $A, B$ be disjoint finite sets. Then $|A \cup B| = |A| + |B|$.

(2) Let $A_1, A_2, \ldots, A_n$ be pairwise disjoint finite sets. Then

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|.$$

**Proof.** Count the elements set by set. Every element in the union is counted exactly once because the sets are (pairwise) disjoint. □

**Theorem 5.3.13** (Inclusion–Exclusion Principle)**.** For all finite sets $A, B$,

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

**Theorem 6.2.1 Some Subset Relations**

1. *Inclusion of Intersection:* For all sets $A$ and $B$,

   (a) $A \cap B \subseteq A$ and (b) $A \cap B \subseteq B$.

2. *Inclusion in Union:* For all sets $A$ and $B$,

   (a) $A \subseteq A \cup B$ and (b) $B \subseteq A \cup B$.

3. *Transitive Property of Subsets:* For all sets $A$, $B$, and $C$,

   if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

**Procedural Versions of Set Definitions**

Let $X$ and $Y$ be subsets of a universal set $U$ and suppose $x$ and $y$ are elements of $U$.

1. $x \in X \cup Y \iff x \in X$ or $x \in Y$
2. $x \in X \cap Y \iff x \in X$ and $x \in Y$
3. $x \in X - Y \iff x \in X$ and $x \notin Y$
4. $x \in X^c \iff x \notin X$
5. $(x, y) \in X \times Y \iff x \in X$ and $y \in Y$

**Definition 6.1.1.** Call $\mathscr{C}$ a *partition* of a set $A$ if

(1) $\mathscr{C}$ is a set of which all elements are *nonempty* subsets of $A$; and

(2) every element of $A$ is in *exactly* one element of $\mathscr{C}$.

Elements of a partition are called *components* of the partition.

**Remark 6.1.2.** One can rewrite the two conditions in the definition of partitions respectively as follows:

(1) $\varnothing \neq S \subseteq A$ for all $S \in \mathscr{C}$;

(2) $\forall x \in A\ \exists S \in \mathscr{C}\ (x \in S)$ and $\forall x \in A\ \forall S_1, S_2 \in \mathscr{C}\ \big(x \in S_1 \wedge x \in S_2 \Rightarrow S_1 = S_2\big)$.

Yet another way to formulate this is to say that $\mathscr{C}$ is a set of mutually disjoint nonempty subsets of $A$ whose union is $A$.

$A_i \cap A_j = \varnothing$, $i \neq j$

**Definition 6.1.5.** Let $A, B$ be sets.

(1) A *relation* from $A$ to $B$ is a subset of $A \times B$.

(2) Let $R$ be a relation from $A$ to $B$ and $(x, y) \in A \times B$. Then we may write

$$x\ R\ y \text{ for } (x, y) \in R \quad \text{and} \quad x\ \not{R}\ y \text{ for } (x, y) \notin R.$$

We read "$x\ R\ y$" as "$x$ is $R$-*related* to $y$" or simply "$x$ is *related* to $y$".

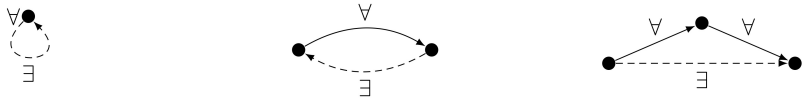



Figure 6.1: Reflexivity, symmetry, and transitivity

**Definition 6.2.1.** A *(binary) relation on a set $A$* is a relation from $A$ to $A$.

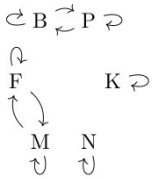
**Remark 6.2.2.** It follows from Definition 6.1.5 and Definition 6.2.1 that the relations on a set $A$ are precisely the subsets of $A \times A$.

**Arrow diagrams (for relations on a set).** One can draw an arrow diagram representing a relation $R$ on a set $A$ as follows.

(1) Draw all the elements of $A$.

(2) For all $x, y \in A$, draw an arrow from $x$ to $y$ if and only if $x\ R\ y$.

**Example 6.2.3.** The arrow diagram




represents the relation

$$\{(\mathrm{B},\mathrm{P}), (\mathrm{P},\mathrm{B}), (\mathrm{F},\mathrm{M}), (\mathrm{M},\mathrm{F}), (\mathrm{B},\mathrm{B}), (\mathrm{P},\mathrm{P}), (\mathrm{F},\mathrm{F}), (\mathrm{M},\mathrm{M}), (\mathrm{K},\mathrm{K}), (\mathrm{E},\mathrm{E})\}$$

on the set $\{\mathrm{B},\mathrm{P},\mathrm{F},\mathrm{M},\mathrm{K},\mathrm{E}\}$.

**Definition 6.2.4.** Let $A$ be a set and $R$ be a relation on $A$.

(1) $R$ is *reflexive* if every element of $A$ is $R$-related to itself, i.e.,

$$\forall x \in A\ \ (x\ R\ x).$$

(2) $R$ is *symmetric* if $x$ is $R$-related to $y$ implies $y$ is $R$-related to $x$, for all $x, y \in A$, i.e.,

$$\forall x, y \in A\ \ (x\ R\ y \Rightarrow y\ R\ x).$$

(3) $R$ is *transitive* if $x$ is $R$-related to $y$ and $y$ is $R$-related to $z$ imply $x$ is $R$-related to $z$, for all $x, y, z \in A$, i.e.,

$$\forall x, y, z \in A\ \ (x\ R\ y \wedge y\ R\ z \Rightarrow x\ R\ z).$$

**Definition 6.2.11.** Let $n, d \in \mathbb{Z}$. Then $d$ is said to *divide $n$* if

$$n = dk \quad \text{for some } k \in \mathbb{Z}.$$

We write $d \mid n$ for "$d$ divides $n$", and $d \nmid n$ for "$d$ does not divide $n$". We also say

"$n$ is *divisible* by $d$" or "$n$ is a *multiple* of $d$" or "$d$ is a *factor/divisor* of $n$"

for "$d$ divides $n$".

**Definition 6.2.13.** An *equivalence relation* is a relation that is reflexive, symmetric and transitive.

**Definition**

Let $R$ be a relation from $A$ to $B$. Define the inverse relation $R^{-1}$ from $B$ to $A$ as follows:

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

This definition can be written operationally as follows:

For all $x \in A$ and $y \in B$, $(y, x) \in R^{-1} \iff (x, y) \in R$.

**Definition**

Given sets $A_1, A_2, \ldots, A_n$, an ***n*-ary relation** $R$ on $A_1 \times A_2 \times \cdots \times A_n$ is a subset of $A_1 \times A_2 \times \cdots \times A_n$. The special cases of 2-ary, 3-ary, and 4-ary relations are called **binary, ternary**, and **quaternary relations**, respectively.

**Definition**

Let $A$ be a set and $R$ a relation on $A$. The **transitive closure** of $R$ is the relation $R^t$ on $A$ that satisfies the following three properties:

1. $R^t$ is transitive.
2. $R \subseteq R^t$.
3. If $S$ is any other transitive relation that contains $R$, then $R^t \subseteq S$.

**Proposition 6.2.16.** Let $\mathscr{C}$ be a partition of a set $A$. Denote by $\sim_{\mathscr{C}}$ the same-component relation with respect to $\mathscr{C}$, i.e., for all $x, y \in A$,

$$\begin{aligned} x \sim_{\mathscr{C}} y &\Leftrightarrow x \text{ is in the same component of } \mathscr{C} \text{ as } y \\ &\Leftrightarrow x, y \in S \text{ for some } S \in \mathscr{C}. \end{aligned}$$

Then $\sim_{\mathscr{C}}$ is an equivalence relation on $A$.

**Proof.** 1. (Reflexivity.) Every element is in the same component as itself.
2. (Symmetry.) If $x$ is in the same component as $y$, then $y$ is in the same component as $x$.
3. (Transitivity.) If $x$ is in the same component as $y$, and $y$ is in the same component as $z$, then $x$ is in the same component as $z$. □

**Definition 6.3.1.** Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. Then *$a$ is congruent to $b$ modulo $n$* if $a - b = nk$ for some $k \in \mathbb{Z}$. In this case, we write $a \equiv b \pmod{n}$.

**Remark 6.3.2.** In terms of divisibility, for all $a, b \in \mathbb{Z}$ and all $n \in \mathbb{Z}^+$,

$$a \equiv b \pmod{n} \quad \Leftrightarrow \quad n \mid (a - b).$$

**Proposition 6.3.4.** Let $n \in \mathbb{Z}^+$ and $\sim_n$ denote the congruence-mod-$n$ relation on $\mathbb{Z}$, i.e., for all $x, y \in \mathbb{Z}$,

$$x \sim_n y \quad \Leftrightarrow \quad x \equiv y \pmod{n}.$$

Then $\sim_n$ is an equivalence relation.

**Proof.** 1. (Reflexivity.) For all $a \in \mathbb{Z}$, we know $a - a = 0 = n \times 0$ and so $a \equiv a \pmod{n}$ by the definition of congruence.

**Definition 6.4.1.** Let $\sim$ be an equivalence relation on a set $A$. For each $x \in A$, the *equivalence class* of $x$ with respect to $\sim$, denoted $[x]_\sim$, is defined to be the set of all elements of $A$ that are $\sim$-related to $x$, i.e.,

$$[x]_\sim = \{y \in A : x \sim y\}.$$

When there is no risk of confusion, we may drop the subscript and write simply $[x]$.

**Lemma 6.4.4.** Let $\sim$ be an equivalence relation on a set $A$. The following are equivalent for all $x, y \in A$.

(i) $x \sim y$.

(ii) $[x] = [y]$.

(iii) $[x] \cap [y] \neq \varnothing$.

**Definition 6.4.6.** Let $A$ be a set and $\sim$ be an equivalence relation on $A$. Denote by $A/\sim$ the set of all equivalence classes with respect to $\sim$, i.e.,

$$A/\sim = \{[x]_\sim : x \in A\}.$$

We may read $A/\sim$ as "the quotient of $A$ by $\sim$".

**Theorem 6.4.9.** Let $\sim$ be an equivalence relation on a set $A$. Then $A/\sim$ is a partition of $A$.

**Proof.** 1. $A/\sim$ is by definition a set.
2. We show that every element of $A/\sim$ is a nonempty subset of $A$.
   2.1. Let $S \in A/\sim$.
   2.2. Use the definition of $A/\sim$ to find $x \in A$ such that $S = [x]$.
   2.3. Then $S = [x] \subseteq A$ in view of the definition of equivalence classes.
   2.4. Note that the reflexivity of $\sim$ implies $x \sim x$.
   2.5. Hence $x \in [x] = S$ by the definition of $[x]$ and the choice of $x$.
   2.6. In particular, we know $S$ is nonempty.
3. We show that every element of $A$ is in at least one element of $A/\sim$.
   3.1. Let $x \in A$.
   3.2. Then $x \sim x$ by reflexivity.
   3.3. So $x \in [x] \in A/\sim$.
4. We show that every element of $A$ is in at most one element of $A/\sim$.
   4.1. Let $x \in A$ that is in two elements of $A/\sim$, say $S_1$ and $S_2$.
   4.2. Use the definition of $A/\sim$ to find $y_1, y_2 \in A$ such that $S_1 = [y_1]$ and $S_2 = [y_2]$.
   4.3. Line 4.1 tells us $x \in [y_1] \cap [y_2]$.
   4.4. So $[y_1] \cap [y_2] \neq \varnothing$.
   4.5. Lemma 6.4.4 then implies $S_1 = [y_1] = [y_2] = S_2$. □

**Definition 7.1.1.** A *representative* of an equivalence class is an element of the equivalence class.

**Definition 7.1.4.** Let $n \in \mathbb{Z}^+$. The quotient $\mathbb{Z}/\sim_n$, where $\sim_n$ is the congruence-mod-$n$ relation on $\mathbb{Z}$, is denoted $\mathbb{Z}_n$ or $\mathbb{Z}/n\mathbb{Z}$. Define addition and multiplication on $\mathbb{Z}_n$ as follows: whenever $[x], [y] \in \mathbb{Z}_n$,

$$[x] + [y] = [x + y] \quad \text{and} \quad [x] \cdot [y] = [x \cdot y].$$

**Proposition 7.1.5.** Addition and multiplication are well defined on $\mathbb{Z}_n$ for all $n \in \mathbb{Z}^+$, i.e., whenever $[x_1], [y_1], [x_2], [y_2] \in \mathbb{Z}_n$,

$$[x_1] = [x_2] \text{ and } [y_1] = [y_2] \quad \Rightarrow \quad [x_1] + [y_1] = [x_2] + [y_2] \text{ and } [x_1] \cdot [y_1] = [x_2] \cdot [y_2].$$

**Definition 7.2.1.** Let $A, B$ be sets. A *function* or a *map* from $A$ to $B$ is an assignment to each element of $A$ exactly one element of $B$. We write $f\colon A \to B$ for "$f$ is a function from $A$ to $B$". Suppose $f\colon A \to B$.

(1) Let $x \in A$. Then $f(x)$ denotes the element of $B$ that $f$ assigns $x$ to. We call $f(x)$ the *image* of $x$ under $f$. If $y = f(x)$, then we say that $f$ *maps $x$ to $y$*, and we may write $f\colon x \mapsto y$.

(2) Here $A$ is called the *domain* of $f$, and $B$ is called the *codomain* of $f$.

**Convention 7.2.2.** Instead of $+(x, y)$ and $\cdot(x, y)$, people usually write $x + y$ and $x \cdot y$ respectively.

**Convention 7.2.3.** In mathematics, one can read

> Define $f\colon A \to B$ by .... Then $f$ is well defined.

as

> The condition "..." defines a function $f\colon A \to B$. We use "..." to define $f$.

Similarly, one can read

> Define $f\colon A \to B$ by .... We show that $f$ is well defined. [Insert proof here.]

as

> We show that the condition "..." defines a function $f\colon A \to B$. [Insert proof here.] We use "..." to define $f$.

**Definition 7.2.5.** Let $A$ be a set. Then the *identity function* on $A$, denoted $\mathrm{id}_A$, is the function $A \to A$ which satisfies, for all $x \in A$,

$$\mathrm{id}_A(x) = x.$$

**Remark 7.2.6.** The domain and the codomain of $\mathrm{id}_A$ are both $A$.

**Definition 7.3.1.** Let $A$ be a set and $R$ be a relation on $A$.

(1) $R$ is *antisymmetric* if $\forall x, y \in A \ \ (x \ R \ y \wedge y \ R \ x \Rightarrow x = y)$.

(2) $R$ is a *(non-strict) partial order* if $R$ is reflexive, antisymmetric, and transitive.

(3) Suppose $R$ is a partial order. Let $x, y \in A$. Then $x, y$ are *comparable (under $R$)* if

$$x \ R \ y \quad \text{or} \quad y \ R \ x.$$

(4) $R$ is a *(non-strict) total order* or a *(non-strict) linear order* if $R$ is a partial order and every pair of elements is comparable, i.e.,

$$\forall x, y \in A \ \ (x \ R \ y \vee y \ R \ x). \quad \text{— also i.e. no branches, just one line.}$$

(5) We say that the ordered pair $(A, R)$ is a *partially ordered set*, or a *poset* for short, if $R$ is a partial order on $A$.

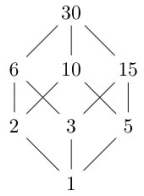
**Note 7.3.2.** A total order is always a partial order.

**Notation 7.3.10.** We often use $\preccurlyeq$ to denote a partial order. This symbol is often defined and redefined to mean different partial orders in different situations. We may read $\preccurlyeq$ as "curly less than or equal to" or simply "less than or equal to" if there is no risk of ambiguity. If $\preccurlyeq$ denotes a partial order, then we write $x \prec y$ for $x \preccurlyeq y \wedge x \neq y$.

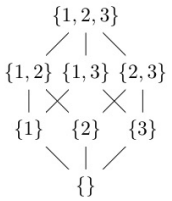
**Definition 7.3.11.** Let $\preccurlyeq$ be a partial order on a set $A$. A *Hasse diagram* of $\preccurlyeq$ satisfies the following condition for all $x, y \in A$:

> If $x \prec y$ and no $z \in A$ is such that $x \prec z \prec y$, then $x$ is placed below $y$ and there is a line joining $x$ to $y$, else no line joins $x$ to $y$.

**Example 7.3.12.** Consider $\{d \in \mathbb{Z}^+ : d \mid 30\}$ partially ordered by the divisibility relation $|$. A Hasse diagram is as follows:




**Example 7.3.13.** Consider $\mathcal{P}(\{1,2,3\})$ partially ordered by the inclusion relation $\subseteq$. A Hasse diagram is as follows:




**Example 7.3.14.** Consider $\{1,2,3,4\}$ partially ordered by the non-strict less-than relation $\leqslant$. A Hasse diagram is as follows:




**Definition 7.4.1.** Let $\preccurlyeq$ be a partial order on a set $A$, and $c \in A$.

(1) $c$ is a *minimal element* if no $x \in A$ is strictly $\preccurlyeq$-less than $c$, i.e.,

$$\forall x \in A \quad (x \preccurlyeq c \Rightarrow c = x).$$

(2) $c$ is a *maximal element* if no $x \in A$ is strictly $\preccurlyeq$-bigger than $c$, i.e.,

$$\forall x \in A \quad (c \preccurlyeq x \Rightarrow c = x).$$

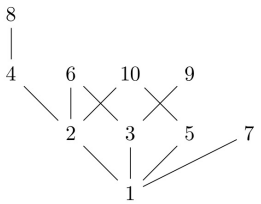
(3) $c$ is the *smallest element* (or the *minimum element*) if all $x \in A$ are $\preccurlyeq$-bigger than or equal to $c$, i.e.,

$$\forall x \in A \quad (c \preccurlyeq x).$$

(4) $c$ is the *largest element* (or the *maximum element*) if all $x \in A$ are $\preccurlyeq$-less than or equal to $c$, i.e.,

$$\forall x \in A \quad (x \preccurlyeq c).$$

**Example 7.4.2.** The divisibility relation $|$ on $\{1, 2, \ldots, 10\}$ is represented by the Hasse diagram




- The only minimal element is 1.
- The maximal elements are $6, 7, 8, 9, 10$.
- The smallest element is 1.
- There is no largest element.

**Proposition 7.4.4.** Consider a partial order $\preccurlyeq$ on a set $A$.

(1) A smallest element is minimal.

(2) There is at most one smallest element.

**Proposition 7.4.6.** With respect to any partial order $\preccurlyeq$ on a nonempty finite set $A$, one can find a minimal element.

**Definition 7.4.8.** Let $A$ be a set and $\preccurlyeq$ be a partial order on $A$. A *linearization* of $\preccurlyeq$ is a total order $\preccurlyeq^*$ on $A$ such that

$$\forall x, y \in A \;\; (x \preccurlyeq y \Rightarrow x \preccurlyeq^* y).$$

**Theorem 7.4.10.** Let $A$ be a set and $\preccurlyeq$ be a partial order on $A$. Then there exists a total order $\preccurlyeq^*$ on $A$ such that for all $x, y \in A$,

$$x \preccurlyeq y \quad \Rightarrow \quad x \preccurlyeq^* y.$$

**Algorithm 7.4.11** (Kahn's Algorithm (1962))**.** Input: a finite set $A$, a partial order $\preccurlyeq$ on $A$.

(1) Set $A_0 := A$ and $i := 0$.

(2) Repeat until $A_i = \varnothing$:

(2.1) use Proposition 7.4.6 to find a minimal element $c_i$ of $A_i$ with respect to $\preccurlyeq$;

(2.2) set $A_{i+1} := A_i \setminus \{c_i\}$;

(2.3) set $i := i + 1$.

Output: a linearization $\preccurlyeq^*$ of $\preccurlyeq$ defined by setting, for all indices $i, j$,

$$c_i \preccurlyeq^* c_j \quad \Leftrightarrow \quad i \leqslant j.$$

**Note 7.4.12.** In step (2.1) of Kahn's Algorithm, there may be several minimal elements to choose from. Different choices give different linearizations.

**Why Kahn's Algorithm stops.** The input set $A$ is finite. Each time the repeat-until loop is run, one element is taken out of $A$. So this loop is run exactly $|A|$ times. Then the set of remaining elements is empty, and the stopping condition is satisfied.

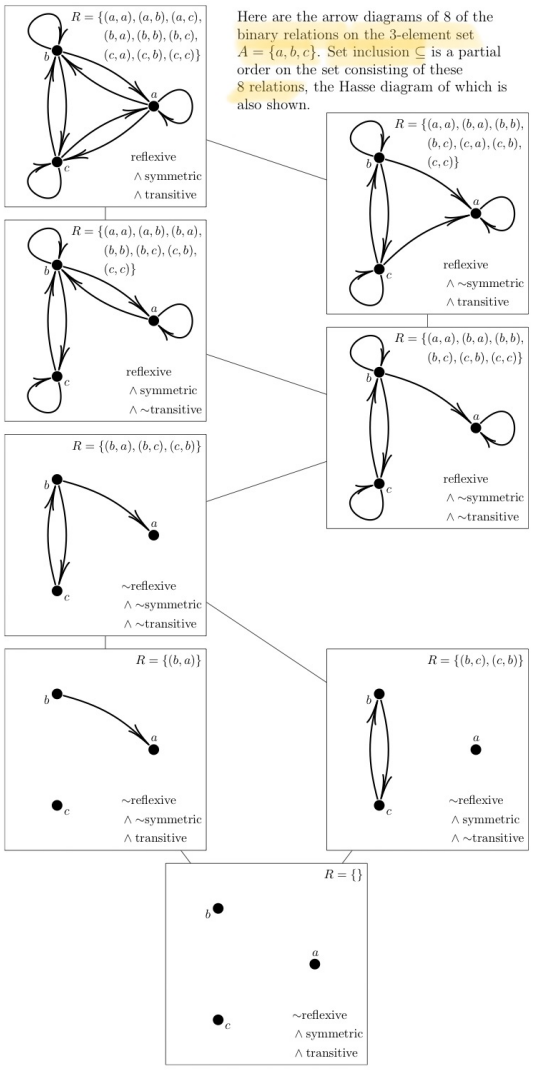



Figure 7.1: A partial order on a set of relations

**Example 8.2.2** **Properties of Equality**

Define a relation $R$ on $\mathbf{R}$ as follows: For all real numbers $x$ and $y$,

$$x \, R \, y \quad \Leftrightarrow \quad x = y.$$

a. Is $R$ reflexive? b. Is $R$ symmetric? c. Is $R$ transitive?

**Solution**

a. ***R is reflexive*:** $R$ is reflexive if, and only if, the following statement is true:

$$\text{For every } x \in \mathbf{R}, \quad x \, R \, x.$$

Since $x \, R \, x$ just means that $x = x$, this is the same as saying

$$\text{For every } x \in \mathbf{R}, \quad x = x.$$

But this statement is certainly true; every real number is equal to itself.

b. ***R is symmetric*:** $R$ is symmetric if, and only if, the following statement is true:

$$\text{For every } x, y \in \mathbf{R}, \quad \text{if } x \, R \, y \text{ then } y \, R \, x.$$





By definition of $R$, $x \, R \, y$ means that $x = y$ and $y \, R \, x$ means that $y = x$. Hence $R$ is symmetric if, and only if,

$$\text{For every } x, y \in \mathbf{R}, \quad \text{if } x = y \text{ then } y = x.$$

But this statement is certainly true; if one number is equal to a second, then the second is equal to the first.

c. ***R is transitive*:** $R$ is transitive if, and only if, the following statement is true:

$$\text{For every } x, y, z \in \mathbf{R}, \quad \text{if } x \, R \, y \text{ and } y \, R \, z \text{ then } x \, R \, z.$$

By definition of $R$, $x \, R \, y$ means that $x = y$, $y \, R \, z$ means that $y = z$, and $x \, R \, z$ means that $x = z$. Hence $R$ is transitive if, and only if, the following statement is true:

$$\text{For every } x, y, z \in \mathbf{R}, \quad \text{if } x = y \text{ and } y = z \text{ then } x = z.$$

But this statement is certainly true: If one real number equals a second and the second equals a third, then the first equals the third. ■

**Theorem 8.4.1 Modular Equivalences**

Let $a$, $b$, and $n$ be any integers and suppose $n > 1$. The following statements are all equivalent:

1. $n \mid (a - b)$
2. $a \equiv b \pmod{n}$
3. $a = b + kn$ for some integer $k$
4. $a$ and $b$ have the same (nonnegative) remainder when divided by $n$
5. $a \bmod n = b \bmod n$

**Proof:** We will show that (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (5) $\Rightarrow$ (1). It will follow by the transitivity of if-then that all five statements are equivalent.

So let $a$, $b$, and $n$ be any integers with $n > 1$.

***Proof that* (1) $\Rightarrow$ (2):** Suppose that $n \mid (a - b)$. By definition of congruence modulo $n$, we can immediately conclude that $a \equiv b \pmod{n}$.

***Proof that* (2) $\Rightarrow$ (3):** Suppose that $a \equiv b \pmod{n}$. By definition of congruence modulo $n$, $n \mid (a - b)$. Thus, by definition of divisibility, $a - b = kn$, for some integer $k$. Adding $b$ to both sides gives that $a = b + kn$.

***Proof that* (3) $\Rightarrow$ (4):** Suppose that $a = b + kn$, for some integer $k$. Use the quotient-remainder theorem to divide $a$ by $n$ to obtain

$$a = qn + r \quad \text{where } q \text{ and } r \text{ are integers and } 0 \le r < n.$$

So $r$ is the remainder obtained when $a$ is divided by $n$. Substituting $b + kn$ for $a$ in the equation $a = qn + r$ gives that

$$b + kn = qn + r,$$

and subtracting $kn$ from both sides and factoring out $n$ yields

$$b = (q - k)n + r.$$

Now since $0 \le r < n$, the uniqueness property of the quotient-remainder theorem guarantees that $r$ is also the remainder obtained when $b$ is divided by $n$. Thus $a$ and $b$ have the same remainder when divided by $n$.

***Proof that* (4) $\Rightarrow$ (5):** Suppose that $a$ and $b$ have the same remainder when divided by $n$. It follows immediately from the definition of the *mod* function that $a \bmod n = b \bmod n$.

***Proof that* (5) $\Rightarrow$ (1):** Suppose that $a \bmod n = b \bmod n$. By definition of the *mod* function, $a$ and $b$ have the same remainder when divided by $n$. Thus, by the quotient-remainder theorem, we can write

$$a = q_1 n + r \quad \text{and} \quad b = q_2 n + r \quad \text{where } q_1, q_2, \text{ and } r \text{ are integers and } 0 \le r < n.$$

It follows that

$$a - b = (q_1 n + r) - (q_2 n + r) = (q_1 - q_2)n.$$

Therefore, since $q_1 - q_2$ is an integer, $n \mid (a - b)$.

**Definition**

Given integers $a$ and $n$ with $n > 1$, **the residue of $a$ modulo $n$** is $a \bmod n$, the nonnegative remainder obtained when $a$ is divided by $n$. The numbers $0, 1, 2, \ldots, n - 1$ are called a **complete set of residues modulo $n$**. To **reduce a number modulo $n$** means to set it equal to its residue modulo $n$. If a modulus $n > 1$ is fixed throughout a discussion and an integer $a$ is given, the words "modulo $n$" are often dropped and we simply speak of **the residue of $a$**.

**Theorem 8.4.2 Congruence Modulo $n$ Is an Equivalence Relation**

If $n$ is any integer with $n > 1$, congruence modulo $n$ is an equivalence relation on the set of all integers. The distinct equivalence classes of the relation are the sets $[0]$, $[1]$, $[2]$, $\ldots$, $[n - 1]$, where for each $a = 0, 1, 2, \ldots, n - 1$,

$$[a] = \{m \in Z \mid m \equiv a \pmod{n}\},$$

or, equivalently,

$$[a] = \{m \in Z \mid m = a + kn \text{ for some integer } k\}.$$

**Proof:** Suppose $n$ is any integer with $n > 1$. We must show that congruence modulo $n$ is reflexive, symmetric, and transitive.

***Proof of reflexivity*:** Suppose $a$ is any integer. To show that $a \equiv a \pmod{n}$, we must show that $n \mid (a - a)$. Now $a - a = 0$, and $n \mid 0$ because $0 = n \cdot 0$. Therefore $a \equiv a \pmod{n}$.

***Proof of symmetry*:** Suppose $a$ and $b$ are any integers such that $a \equiv b \pmod{n}$. We must show that $b \equiv a \pmod{n}$. Now since $a \equiv b \pmod{n}$, then $n \mid (a - b)$. Thus, by definition of divisibility, $a - b = nk$, for some integer $k$. Multiply both sides of this equation by $-1$ to obtain

$$-(a - b) = -nk,$$

or, equivalently,

$$b - a = n(-k).$$

Thus, by definition of divisibility $n \mid (b - a)$, and so, by definition of congruence modulo $n$, $b \equiv a \pmod{n}$.

***Proof of transitivity*:** This is left as exercise 5 at the end of the section.

***Proof that the distinct equivalence classes are* [0], [1], [2], . . . , [$n$ − 1]:** This is left as exercise 6 at the end of the section.

**Corollary 8.4.4**

Let $a$, $b$, and $n$ be integers with $n > 1$. Then

$$ab \equiv [(a \bmod n)(b \bmod n)] \pmod{n},$$

or, equivalently,

$$ab \bmod n = [(a \bmod n)(b \bmod n)] \bmod n.$$

In particular, if $m$ is a positive integer, then

$$a^m \equiv [(a \bmod n)^m] \pmod{n}.$$

**Theorem 8.4.3 Modular Arithmetic**

Let $a$, $b$, $c$, $d$, and $n$ be integers with $n > 1$, and suppose

$$a \equiv c \pmod{n} \quad \text{and} \quad b \equiv d \pmod{n}.$$

Then

1. $(a + b) \equiv (c + d) \pmod{n}$
2. $(a - b) \equiv (c - d) \pmod{n}$
3. $ab \equiv cd \pmod{n}$
4. $a^m \equiv c^m \pmod{n}$ for every positive integer $m$.

**Proof:** Because we will make greatest use of part 3 of this theorem, we prove it here and leave the proofs of the remaining parts of the theorem to exercises 9–11 at the end of the section.

***Proof of Part 3*:** Suppose $a$, $b$, $c$, $d$, and $n$ are integers with $n > 1$, and suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. By Theorem 8.4.1, there exist integers $s$ and $t$ such that

$$a = c + sn \quad \text{and} \quad b = d + tn.$$

Then

$$\begin{aligned} ab &= (c + sn)(d + tn) && \text{by substitution} \\ &= cd + ctn + snd + sntn \\ &= cd + n(ct + sd + stn) && \text{by algebra.} \end{aligned}$$

Let $k = ct + sd + stn$. Then $k$ is an integer because it is a sum of products of integers, and $ab = cd + nk$. Thus by Theorem 8.4.1, $ab \equiv cd \pmod{n}$.

**Definition**

An integer $d$ is said to be a **linear combination of integers** $a$ and $b$ if, and only if, there exist integers $s$ and $t$ such that $as + bt = d$.

**Theorem 8.4.5 Writing a Greatest Common Divisor as a Linear Combination**

For all integers $a$ and $b$, not both zero, if $d = \gcd(a, b)$, then there exist integers $s$ and $t$ such that $as + bt = d$.

**Proof:** Given integers $a$ and $b$, not both zero, and given $d = \gcd(a, b)$, let

$$S = \{x \mid x \text{ is a positive integer and } x = as + bt \text{ for some integers } s \text{ and } t\}.$$

Note that $S$ is a nonempty set because (1) if $a > 0$ then $1 \cdot a + 0 \cdot b \in S$, (2) if $a < 0$ then $(-1) \cdot a + 0 \cdot b \in S$, and (3) if $a = 0$ then, by assumption, $b \neq 0$, and hence $0 \cdot a + 1 \cdot b \in S$ or $0 \cdot a + (-1) \cdot b \in S$. Thus, because $S$ is a nonempty subset of positive integers, by the well-ordering principle for the integers there is a least element $c$ in $S$. By definition of $S$,

$$c = as + bt \quad \text{for some integers } s \text{ and } t. \tag{8.4.3}$$

We will show that (1) $c \geq d$, and (2) $c \leq d$, and we will therefore be able to conclude that $c = d = \gcd(a, b)$.

**(1) *Proof that $c \geq d$:***

*[In this part of the proof, we show that $d$ is a divisor of $c$ and thus that $d \leq c$.]* Because $d = \gcd(a, b)$, by definition of greatest common divisor, $d \mid a$ and $d \mid b$. Hence $a = dx$ and $b = dy$ for some integers $x$ and $y$. Then

$$\begin{aligned} c &= as + bt && \text{by (8.4.3)} \\ &= (dx)s + (dy)t && \text{by substitution} \\ &= d(xs + y) && \text{by factoring out the } d. \end{aligned}$$

Now $xs + yt$ is an integer because it is a sum of products of integers. Thus, by definition of divisibility, $d \mid c$. Both $c$ and $d$ are positive, and hence, by Theorem 4.4.1, $c \geq d$.

**(2) *Proof that $c \leq d$:***

*[In this part of the proof, we show that $c$ is a divisor of both $a$ and $b$ and therefore that $c$ is less than or equal to the greatest common divisor of $a$ and $b$, which is $d$.]* Apply the quotient-remainder theorem to the division of $a$ by $c$ to obtain

$$a = cq + r \quad \text{for some integers } q \text{ and } r \text{ with } 0 \leq r < c. \tag{8.4.4}$$

Thus for some integers $q$ and $r$ with $0 \leq r < c$,

$$r = a - cq.$$

Now $c = as + bt$. Therefore, for some integers $q$ and $r$ with $0 \leq r < c$,

$$\begin{aligned} r &= a - (as + bt)q && \text{by substitution.} \\ &= a(1 - sq) - btq \end{aligned}$$

Thus $r$ is a linear combination of $a$ and $b$. If $r > 0$, then $r$ would be in $S$, and so $r$ would be a smaller element of $S$ than $c$, which would contradict the fact that $c$ is the least element of $S$. Hence $r = 0$. By substitution into (8.4.4),

$$a = cq$$

and therefore $c \mid a$.

An almost identical argument establishes that $c \mid b$ and is left as exercise 30 at the end of the section.

Because $c \mid a$ and $c \mid b$, $c$ is a common divisor of $a$ and $b$. Hence $c$ is less than or equal to the greatest common divisor of $a$ and $b$. In other words, $c \leq d$.

From (1) and (2), we conclude that $c = d$. It follows that $d$, the greatest common divisor of $a$ and $b$, is equal to $as + bt$.

**Definition**

Given any integer $a$ and any positive integer $n$, if there exists an integer $s$ such that $as \equiv 1 \pmod{n}$, then $s$ is called **an inverse for $a$ modulo $n$**.

Unfortunately, the method shown above cannot always be used to solve congruences because not every integer has an inverse modulo $n$. For instance, observe that

$$2 \cdot 1 \equiv 2 \pmod 4$$
$$2 \cdot 2 \equiv 0 \pmod 4$$
$$2 \cdot 3 \equiv 2 \pmod 4.$$

By Theorem 8.4.3, these calculations suffice to show that the number 2 does not have an inverse modulo 4.

Describing the circumstances in which inverses exist in modular arithmetic requires the concept of relative primeness.

**Definition**

Integers $a$ and $b$ are **relatively prime** if, and only if, $\gcd(a, b) = 1$. Integers $a_1, a_2, a_3, \ldots, a_n$ are **pairwise relatively prime** if, and only if, $\gcd(a_i, a_j) = 1$ for all integers $i$ and $j$ with $1 \le i, j \le n$, and $i \ne j$.

Given the definition of relatively prime integers, the following corollary is an immediate consequence of Theorem 8.4.5.

**Corollary 8.4.6**

If $a$ and $b$ are relatively prime integers, then there exist integers $s$ and $t$ such that $as + bt = 1$.

**Theorem 8.4.8 Euclid's Lemma**

For all integers $a$, $b$, and $c$, if $\gcd(a, c) = 1$ and $a \mid bc$, then $a \mid b$.

**Proof:** Suppose $a$, $b$, and $c$ are integers, $\gcd(a, c) = 1$, and $a \mid bc$. *[We must show that $a \mid b$.]* By Theorem 8.4.5, there exist integers $s$ and $t$ so that

$$as + ct = 1.$$

Multiply both sides of this equation by $b$ to obtain

$$bas + bct = b. \qquad 8.4.7$$

Since $a \mid bc$, by definition of divisibility there exists an integer $k$ such that

$$bc = ak. \qquad 8.4.8$$

Substituting (8.4.8) into (8.4.7), rewriting, and factoring out an $a$ gives that

$$b = bas + (ak)t = a(bs + kt).$$

Let $r = bs + kt$. Then $r$ is an integer (because $b$, $s$, $k$, and $t$ are all integers), and $b = ar$. Thus $a \mid b$ by definition of divisibility.

The unique factorization theorem for the integers states that any integer greater than 1 has a unique representation as a product of prime numbers, except possibly for the order in which the numbers are written. The hint for exercise 13 of Section 5.4 outlined a proof of the existence part of the proof, and the uniqueness of the representation follows quickly from Euclid's lemma. In exercise 41 at the end of this section, we outline a proof for you to complete.

Another application of Euclid's lemma is a cancellation theorem for congruence modulo $n$. This theorem allows us—under certain circumstances—to divide out a common factor in a congruence relation.

**Theorem 8.4.9 Cancellation Theorem for Modular Congruence**

For all integers $a$, $b$, $c$, and $n$ with $n > 1$, if $\gcd(c, n) = 1$ and $ac \equiv bc \pmod n$, then $a \equiv b \pmod n$.

*(continued on page 540)*

**Corollary 8.4.7 Existence of Inverses Modulo $n$**

For all integers $a$ and $n$, if $\gcd(a, n) = 1$, then there exists an integer $s$ such that $as \equiv 1 \pmod n$, and so $s$ is an inverse for $a$ modulo $n$.

**Proof:** Suppose $a$ and $n$ are integers and $\gcd(a, n) = 1$. By Corollary 8.4.6, there exist integers $s$ and $t$ such that

$$as + nt = 1.$$

Subtracting $nt$ from both sides gives that

$$as = 1 - nt = 1 + (-t)n.$$

Thus, by definition of congruence modulo $n$,

$$as \equiv 1 \pmod n.$$

part 2

# CS1231S Chapter 8

# Induction and recursion

## 8.1 Mathematical Induction

**Principle 8.1.1** (Mathematical Induction (MI))**.** Let $m \in \mathbb{Z}$. To prove that $\forall n \in \mathbb{Z}_{\geqslant m}\ P(n)$ is true, where each $P(n)$ is a proposition, it suffices to:

**(base step)** show that $P(m)$ is true; and

**(induction step)** show that $\forall k \in \mathbb{Z}_{\geqslant m}\ \big(P(k) \Rightarrow P(k+1)\big)$ is true.

**Justification.** The two steps ensure the following are true:

| | |
|---|---|
| $P(m)$ | by the base step; |
| $P(m) \Rightarrow P(m+1)$ | by the induction step with $k = m$; |
| $P(m+1) \Rightarrow P(m+2)$ | by the induction step with $k = m+1$; |
| $P(m+2) \Rightarrow P(m+3)$ | by the induction step with $k = m+2$; |
| $\vdots$ | |

We deduce that $P(m), P(m+1), P(m+2), \ldots$ are all true by a series of modus ponens. □

**Terminology 8.1.2.** In the induction step, we assume we have $k \in \mathbb{Z}_{\geqslant m}$ such that $P(k)$ is true, and then show $P(k+1)$ using this assumption. In this process, the assumption that $P(k)$ is true is called the *induction hypothesis*.

**Example 8.1.3.** $1 + 2 + \cdots + n = \frac{1}{2}\, n(n+1)$ for all $n \in \mathbb{Z}_{\geqslant 1}$.

**Proof.** 1. For each $n \in \mathbb{Z}_{\geqslant 1}$, let $P(n)$ be the proposition "$1 + 2 + \cdots + n = \frac{1}{2}\, n(n+1)$".
2. (Base step) $P(1)$ is true because $1 = \frac{1}{2} \times 1 \times (1+1)$.
3. (Induction step)
   3.1. Let $k \in \mathbb{Z}_{\geqslant 1}$ such that $P(k)$ is true, i.e., such that

$$1 + 2 + \cdots + k = \frac{1}{2}\, k(k+1).$$

   3.2. Then $1 + 2 + \cdots + k + (k+1)$
   3.3. $= \frac{1}{2}\, k(k+1) + (k+1)$ by the induction hypothesis $P(k)$;
   3.4. $= \left(\frac{k}{2} + 1\right)(k+1) = \frac{k+2}{2}\,(k+1)$
   3.5. $= \frac{1}{2}\,(k+1)((k+1)+1)$.
   3.6. So $P(k+1)$ is true.

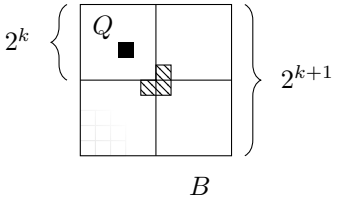



Figure 8.1: Covering a checkerboard with L-trominos

4. Hence $\forall n \in \mathbb{Z}_{\geqslant 1}$ $P(n)$ is true by MI. □

**Terminology 8.1.4.** We call the proof above an induction *on* $n$ because $n$ is the active variable in it.

**Example 8.1.5.** $n! > 2^n$ for all $n \in \mathbb{Z}_{\geqslant 4}$, where $n! = n \times (n-1) \times \cdots \times 1$.

**Proof.** 1. For each $n \in \mathbb{Z}_{\geqslant 4}$, let $P(n)$ be the proposition "$n! > 2^n$".
2. (Base step) $P(4)$ is true because $4! = 24 > 16 = 2^4$.
3. (Induction step)
   3.1. Let $k \in \mathbb{Z}_{\geqslant 4}$ such that $P(k)$ is true, i.e., such that
   $$k! > 2^k.$$
   3.2. Then $(k+1)! = (k+1) \times k!$ by the definition of !;
   3.3. $> (k+1) \times 2^k$ by the induction hypothesis $P(k)$;
   3.4. $> 2 \times 2^k$ as $k + 1 \geqslant 4 + 1 > 2$;
   3.5. $= 2^{k+1}$.
   3.6. So $P(k+1)$ is true.
4. Hence $\forall n \in \mathbb{Z}_{\geqslant 4}$ $P(n)$ is true by MI. □

**Example 8.1.6.** An *L-tromino* is the following L-shape formed by three squares of the checkerboard:

For all $n \in \mathbb{Z}_{\geqslant 1}$, if one square is removed from a $2^n \times 2^n$ checkerboard, then the remaining squares can be covered by L-trominos.

**Proof.** 1. For each $n \in \mathbb{Z}_{\geqslant 1}$, let $P(n)$ be the proposition

> if one square is removed from a $2^n \times 2^n$ checkerboard, then the remaining squares can be covered by L-trominos.

2. (Base step) $P(1)$ is true because such a board itself is an L-tromino.
3. (Induction step)
   3.1. Let $k \in \mathbb{Z}_{\geqslant 1}$ such that $P(k)$ is true.
   3.2. 3.2.1. Let $B$ be a $2^{k+1} \times 2^{k+1}$ checkerboard with one square removed.
   3.2.2. Divide $B$ into four $2^k \times 2^k$ quadrants.
   3.2.3. Let $Q$ be the quadrant containing the removed square.
   3.2.4. Remove one L-tromino from the centre of $B$ in a way such that each quadrant other than $Q$ has one square removed.
   3.2.5. We are left with four $2^k \times 2^k$ checkerboards, each with one square removed.
   3.2.6. By the induction hypothesis, each quadrant can be covered by L-trominos.
   3.2.7. Hence $B$ can be covered by L-trominos.
   3.3. This shows $P(k+1)$ is true.
4. Hence $\forall n \in \mathbb{Z}_{\geqslant 1}$ $P(n)$ is true by MI. □

**Example 8.1.7.** All participants in this Zoom meeting have the same birthday. 8a

**Proof.** 1. For each $n \in \mathbb{Z}_{\geqslant 1}$, let $P(n)$ be the proposition

if a Zoom meeting has exactly $n$ participants, then all its participants have the same birthday.

2. (Base step) $P(1)$ is true because if a Zoom meeting has exactly 1 participant, then clearly all its participants have the same birthday.
3. (Induction step)
   - 3.1. Let $k \in \mathbb{Z}_{\geqslant 1}$ such that $P(k)$ is true.
   - 3.2. 3.2.1. Suppose a Zoom meeting has exactly $k+1$ participants.
     - 3.2.2. Pick two different participants $a, b$ in the meeting.
     - 3.2.3. Ask $a$ to leave the meeting.
     - 3.2.4. Since there are $k$ people left in the meeting, by the induction hypothesis, all the remaining participants have the same birthday, including $b$.
     - 3.2.5. Tell $a$ to join the meeting again, and then ask $b$ to leave the meeting.
     - 3.2.6. Since there are $k$ people left in the meeting, by the induction hypothesis, all the remaining participants have the same birthday, including $a$.
     - 3.2.7. The participants who stayed in the meeting throughout have the same birthday as both $a$ and $b$.
     - 3.2.8. So $a$ and $b$ have the same birthday.
   - 3.3. This shows $P(k+1)$ is true.
4. Hence $\forall n \in \mathbb{Z}_{\geqslant 1}\ \ P(n)$ is true by MI. ⊠

## 8.2 Strong Mathematical Induction

**Principle 8.2.1** (Strong Mathematical Induction (Strong MI))**.** To prove that $\forall n \in \mathbb{Z}_{\geqslant m}\ \ P(n)$ is true, where each $P(n)$ is a proposition and $m \in \mathbb{Z}$, it suffices to choose some $\ell \in \mathbb{Z}_{\geqslant 0}$ and:

**(base step)** show that $P(m), P(m+1), \ldots, P(m+\ell-1)$ are true;

**(induction step)** show that

$$\forall k \in \mathbb{Z}_{\geqslant 0}\ \ \big(P(m) \wedge P(m+1) \wedge \cdots \wedge P(m+\ell-1+k) \Rightarrow P(m+\ell+k)\big)$$

is true.

**Justification.** The two steps ensure the following are true:

$$P(m) \wedge P(m+1) \wedge \cdots \wedge P(m+\ell-1)$$
by the base step;
$$P(m) \wedge P(m+1) \wedge \cdots \wedge P(m+\ell-1) \Rightarrow P(m+\ell)$$
by the induction step with $k=0$;
$$P(m) \wedge P(m+1) \wedge \cdots \wedge P(m+\ell-1) \wedge P(m+\ell) \Rightarrow P(m+\ell+1)$$
by the induction step with $k=1$;
$$P(m) \wedge P(m+1) \wedge \cdots \wedge P(m+\ell-1) \wedge P(m+\ell) \wedge P(m+\ell+1) \Rightarrow P(m+\ell+2)$$
by the induction step with $k=2$;
$$\vdots$$

We deduce that $P(m), P(m+1), P(m+2), P(m+3), \ldots$ are all true by a series of modus ponens. □

**Definition 8.2.2.** The *Fibonacci sequence* $F_0, F_1, F_2, \ldots$ is defined by setting

$$F_0 = 0 \quad \text{and} \quad F_1 = 1 \quad \text{and} \quad F_{n+2} = F_{n+1} + F_n$$

for each $n \in \mathbb{Z}_{\geqslant 0}$.

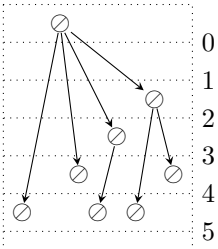



Figure 8.2: Rabbits

**Example 8.2.3.** $F_2 = 1+0 = 1, \quad F_3 = 1+1 = 2, \quad F_4 = 2+1 = 3, \quad F_5 = 3+2 = 5, \quad \ldots.$

**Example 8.2.4.**

- Initially, there is one pair of newly born matched rabbits.
- Each newly born rabbit takes one month to mature.
- Each mature pair of matched rabbits produces one pair of matched rabbits per month.

Let $r_n$ denote the number of pairs of rabbits after $n$ months. Then for every $n \in \mathbb{Z}_{\geqslant 0}$,

$$r_0 = 1 \quad \text{and} \quad r_1 = 1 \quad \text{and} \quad r_{n+2} = r_{n+1} + r_n,$$

where the $r_{n+1}$ comes from the rabbits already present after $(n+1)$ months, and the $r_n$ comes from the rabbits born after $(n+1)$ months.

**Observation 8.2.5.** $r_n = F_{n+1}$ for every $n \in \mathbb{Z}_{\geqslant 0}$.

**Example 8.2.6.** $F_{n+1} \leqslant (7/4)^n$ for every $n \in \mathbb{Z}_{\geqslant 0}$.

**Proof.** 1. For each $n \in \mathbb{Z}_{\geqslant 0}$, let $P(n)$ be the proposition "$F_{n+1} \leqslant (7/4)^n$".
2. (Base step) $P(0)$ and $P(1)$ are true because

$$F_{0+1} = 1 \leqslant 1 = (7/4)^0 \quad \text{and} \quad F_{1+1} = 1+0 = 1 \leqslant 7/4 = (7/4)^1.$$

3. (Induction step)
   3.1. Let $k \in \mathbb{Z}_{\geqslant 0}$ such that $P(0), P(1), \ldots, P(k+1)$ are true.
   3.2. Then $F_{(k+2)+1} = F_{k+3}$
   3.3. $= F_{k+2} + F_{k+1}$ by the definition of $F_{k+3}$;
   3.4. $\leqslant (7/4)^{k+1} + (7/4)^k$ as $P(k)$ and $P(k+1)$ are true;
   3.5. $= (7/4)^k(7/4+1)$
   3.6. $< (7/4)^k(7/4)^2$ as $7/4+1 = 11/4 < 49/16 = (7/4)^2$;
   3.7. $= (7/4)^{k+2}$.
   3.8. So $P(k+2)$ is true.
4. Hence $\forall n \in \mathbb{Z}_{\geqslant 0}$ $P(n)$ is true by Strong MI. □

**Remark 8.2.7.** Given the same $P(n)$, Strong MI is more likely to succeed than usual MI, but the proof may be more cumbersome when written.

**Remark 8.2.8.** When $\ell = 0$ in Principle 8.2.1 (Strong MI), the base step is empty. Thus to prove that $\forall n \in \mathbb{Z}_{\geqslant m}$ $P(n)$ is true, where each $P(n)$ is a proposition and $m \in \mathbb{Z}$, it suffices to show *only*

$$\forall k \in \mathbb{Z}_{\geqslant 0} \quad \big(P(m) \wedge P(m+1) \wedge \cdots \wedge P(m+k-1) \Rightarrow P(m+k)\big).$$

(The conjunction of no formula is by convention always true.)

**Example 8.2.9.** (1) $S = \{x \in \mathbb{Z}_{\geqslant 0} : 0 < x < 5\}$ has smallest element 1.

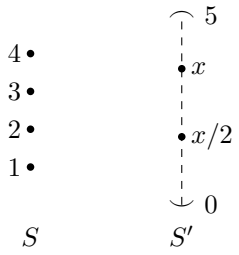



Figure 8.3: A difference between $\mathbb{Z}_{\geqslant 0}$ and $\mathbb{Q}_{\geqslant 0}$

(2) $S' = \{x \in \mathbb{Q}_{\geqslant 0} : 0 < x < 5\}$ has no smallest element because if $x \in S'$, then $x/2 \in S'$ and $x/2 < x$.

**Theorem 8.2.10** (Well-Ordering Principle)**.** Every nonempty subset of $\mathbb{Z}_{\geqslant m}$, where $m \in \mathbb{Z}$, has a smallest element.

**Proof.** We prove this by Principle 8.2.1 (Strong MI) with $\ell = 0$.
1. Let $m \in \mathbb{Z}$ and $S \subseteq \mathbb{Z}_{\geqslant m}$ with no smallest element.
2. For each $n \in \mathbb{Z}_{\geqslant m}$, let $P(n)$ be the proposition " $n \notin S$ ".
3. (Induction step)
   - 3.1. Let $k \in \mathbb{Z}_{\geqslant 0}$ such that $P(m), P(m+1), \ldots, P(m+k-1)$ are true, i.e., that $m, m+1, \ldots, m+k-1 \notin S$.
   - 3.2. 3.2.1. Suppose $m + k \in S$.
     - 3.2.2. Then $m + k$ is the smallest element of $S$ by the induction hypothesis as $S \subseteq \mathbb{Z}_{\geqslant m}$.
     - 3.2.3. This contradicts our assumption that $S$ has no smallest element on line 1.
   - 3.3. So $m + k \notin S$.
   - 3.4. Thus $P(m + k)$ is true.
4. Hence $\forall n \in \mathbb{Z}_{\geqslant m}$ $P(n)$ is true by Strong MI.
5. This implies $S = \varnothing$ as $S \subseteq \mathbb{Z}_{\geqslant m}$. □

## 8.3 Recursively defined sequences

**Terminology 8.3.1.** A sequence $a_0, a_1, a_2, \ldots$ is said to be *recursively defined* if the definition of $a_n$ involves $a_0, a_1, \ldots, a_{n-1}$ for all but finitely many $n \in \mathbb{Z}_{\geqslant 0}$.

**Example 8.3.2.** (1) Define $0!, 1!, 2!, \ldots$ by setting, for each $n \in \mathbb{Z}_{\geqslant 0}$,

$$0! = 1 \quad \text{and} \quad (n+1)! = (n+1) \times n!.$$

Then $1! = 1 \times 1 = 1$, $2! = 2 \times 1 = 2$, $3! = 3 \times 2 = 6$, $4! = 4 \times 6 = 24$, ....

(2) The *Fibonacci sequence* $F_0, F_1, F_2, \ldots$ was defined in Definition 8.2.2 by setting, for each $n \in \mathbb{Z}_{\geqslant 0}$,

$$F_0 = 0 \quad \text{and} \quad F_1 = 1 \quad \text{and} \quad F_{n+2} = F_{n+1} + F_n.$$

Then $F_2 = 1 + 0 = 1$, $F_3 = 1 + 1 = 2$, $F_4 = 2 + 1 = 3$, $F_5 = 3 + 2 = 5$, ....

(3) Fix $r \in [0, 4]$ and $p_0 \in [0, 1]$. Define $p_1, p_2, \ldots$ by setting, for each $n \in \mathbb{Z}_{\geqslant 0}$,

$$p_{n+1} = r(p_n - {p_n}^2).$$

If $r = 3$ and $p_0 = 1/2$, then

$$p_1 = 3\Big(\frac{1}{2} - \Big(\frac{1}{2}\Big)^2\Big) = \frac{3}{4}, \quad p_2 = 3\Big(\frac{3}{4} - \Big(\frac{3}{4}\Big)^2\Big) = \frac{9}{16}, \quad \ldots.$$

(4) Fix $a_0 \in \mathbb{Z}^+$. Define $a_1, a_2, a_3, \ldots$ by setting, for each $n \in \mathbb{Z}_{\geqslant 0}$,

$$a_{n+1} = \begin{cases} a_n/2, & \text{if } a_n \text{ is even;} \\ 3a_n + 1, & \text{if } a_n \text{ is odd.} \end{cases}$$

If $a_0 = 1$, then $a_1 = 3 \times 1 + 1 = 4, \quad a_2 = 4/2 = 2, \quad a_3 = 2/2 = 1, \quad \ldots$.

**Exercise 8.3.3.** Let $a_1 = 1$ and $a_{n+1} = a_n + (n+1)$ for all $n \in \mathbb{Z}_{\geqslant 1}$. Find a general formula for $a_n$ in terms of $n$ that does not involve $a_0, a_1, \ldots, a_{n-1}$. 8b

**Proposition 8.3.4.** There is a unique sequence $a_0, a_1, a_2, \ldots$ satisfying, for each $n \in \mathbb{Z}_{\geqslant 0}$,

$$a_0 = 0 \quad \text{and} \quad a_1 = 1 \quad \text{and} \quad a_{n+2} = a_{n+1} + a_n.$$

**Proof (optional material).** For the purpose of this proof, let us call a sequence $b_0, b_1, \ldots, b_{n-1}$ a *partial sequence* if for all $i \in \mathbb{Z}_{\geqslant 0}$ with $i < n$,

$$b_i = \begin{cases} 0, & \text{if } i = 0; \\ 1, & \text{if } i = 1; \\ b_{i-1} + b_{i-2}, & \text{if } i \geqslant 2. \end{cases}$$

1. First, we claim that there is a partial sequence of length $n$ for every $n \in \mathbb{Z}_{\geqslant 0}$.
   1.1. For each $n \in \mathbb{Z}_{\geqslant 0}$, let $P(n)$ be the proposition

   "there is a partial sequence of length $n$".

   1.2. (Base step) $P(0)$ is true because the empty sequence is trivially a partial sequence of length 0.
   1.3. (Induction step)
      1.3.1. Let $k \in \mathbb{Z}_{\geqslant 0}$ such that $P(k)$ is true.
      1.3.2. This gives a partial sequence $b_0, b_1, \ldots, b_{k-1}$ of length $k$.
      1.3.3. Define

      $$b_k = \begin{cases} 0, & \text{if } k = 0; \\ 1, & \text{if } k = 1; \\ b_{k-1} + b_{k-2}, & \text{if } k \geqslant 2. \end{cases}$$

      1.3.4. Then $b_0, b_1, \ldots, b_k$ is a partial sequence of length $k+1$ by the choice of $b_k$ and because $b_0, b_1, \ldots, b_{k-1}$ is a partial sequence.
      1.3.5. So $P(k+1)$ is true.
   1.4. Hence $\forall n \in \mathbb{Z}_{\geqslant 0}$ $P(n)$ is true by MI.
2. If $b_0, b_1, \ldots, b_{m-1}$ and $c_0, c_1, \ldots, c_{n-1}$ are partial sequences with $m \leqslant n$, then

$$\begin{aligned} b_0 &= 0 = c_0, \\ b_1 &= 1 = c_1, \\ b_2 = b_1 + b_0 &= c_1 + c_0 = c_2, \\ b_3 = b_2 + b_1 &= c_2 + c_1 = c_3, \\ &\vdots \\ b_{m-1} = b_{m-2} + b_{m-3} &= c_{m-2} + c_{m-3} = c_{m-1}. \end{aligned}$$

3. For each $n \in \mathbb{Z}_{\geqslant 0}$, define $a_n$ to be the $n$th element of any partial sequence of length at least $n$.
4. Then the sequence $a_0, a_1, a_2, \ldots$ is well defined by lines 1 and 2.
5. This sequence $a_0, a_1, a_2, \ldots$ is what we want because it agrees with all the partial sequences, and the conditions in the definition of partial sequences match with the required conditions.

6. Let $b_0, b_1, b_2, \ldots$ be a sequence satisfying, for each $n \in \mathbb{Z}_{\geqslant 0}$,

$$b_0 = 0 \quad \text{and} \quad b_1 = 1 \quad \text{and} \quad b_{n+2} = b_{n+1} + b_n.$$

7. We show that $a_n = b_n$ for all $n \in \mathbb{Z}_{\geqslant 0}$.
   7.1. Let $n \in \mathbb{Z}_{\geqslant 0}$.
   7.2. Note that $a_0, a_1, \ldots, a_n$ and $b_0, b_1, \ldots, b_n$ are partial sequences.
   7.3. So $a_n = b_n$ by line 2. □

## 8.4 Recursively defined sets

**Theorem 8.4.1.** $\mathbb{Z}_{\geqslant 0}$ is the unique set with the following properties.

(1) $0 \in \mathbb{Z}_{\geqslant 0}$. (base clause)

(2) If $x \in \mathbb{Z}_{\geqslant 0}$, then $x + 1 \in \mathbb{Z}_{\geqslant 0}$. (recursion clause)

(3) Membership for $\mathbb{Z}_{\geqslant 0}$ can always be demonstrated by (finitely many) successive applications of the clauses above. (minimality clause)

**Example 8.4.2.**

$0 \in \mathbb{Z}_{\geqslant 0}$ by (1).
$\therefore\ 1 \in \mathbb{Z}_{\geqslant 0}$ by (2) and the previous line.
$\therefore\ 2 \in \mathbb{Z}_{\geqslant 0}$ by (2) and the previous line.

**Remark 8.4.3.** (1) and (2) are true when $\mathbb{Z}_{\geqslant 0}$ is changed to $\mathbb{Q}$, but (3) is not. So (1) and (2) are not enough to uniquely determine $\mathbb{Z}_{\geqslant 0}$.

**Terminology 8.4.4.** Theorem 8.4.1 gives a *recursive definition* of $\mathbb{Z}_{\geqslant 0}$.

**Rough idea 8.4.5.** A recursive definition of a set $S$ consists of three types of clauses.

**(base clause)** Specify that certain elements, called *founders*, are in $S$: if $c$ is a founder, then $c \in S$.

**(recursion clause)** Specify certain functions, called *constructors*, under which the set $S$ is closed: if $f$ is a constructor and $x \in S$, then $f(x) \in S$.

**(minimality clause)** Membership for $S$ can always be demonstrated by (finitely many) successive applications of the clauses above.

In words, the members of $S$ are precisely those objects that can be obtained from the founders by successively applying the constructors.

**Rough idea 8.4.6** (structural induction)**.** Let $S$ be a recursively defined set. To prove that $\forall x \in S \ \ P(x)$ is true, where each $P(x)$ is a proposition, it suffices to:

**(base step)** show that $P(c)$ is true for every founder $c$;

**(induction step)** show that $\forall x \in S \ \ \big(P(x) \Rightarrow P(f(x))\big)$ is true for every constructor $f$.

In words, if all the founders satisfy a property $P$, and $P$ is preserved by all constructors, then all elements of $S$ satisfy $P$.

**Example 8.4.7.** The set $2\mathbb{Z}$ of all even integers can be defined recursively as follows.

(1) $0 \in S$. (base clause)

(2) If $x \in S$, then $x - 2 \in 2\mathbb{Z}$ and $x + 2 \in 2\mathbb{Z}$. (recursion clause)

(3) Membership for $2\mathbb{Z}$ can always be demonstrated by (finitely many) successive applications of clauses above. (minimality clause)

**Theorem 8.4.8** (Structural induction over $2\mathbb{Z}$)**.** To prove that $\forall n \in 2\mathbb{Z}\ \ P(n)$ is true, where each $P(n)$ is a proposition, it suffices to:

**(base step)** show that $P(0)$ is true; and

**(induction step)** show that $\forall x \in 2\mathbb{Z}\ \ \big(P(x) \Rightarrow P(x-2) \wedge P(x+2)\big)$ is true.

**Question 8.4.9.** Define a set $S$ recursively as follows. 8c

(1) $1 \in S$. (base clause)

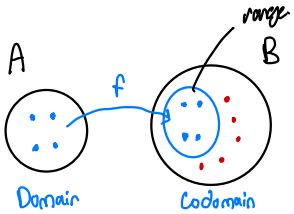
(2) If $x \in S$, then $2x \in S$ and $3x \in S$. (recursion clause)

(3) Membership for $S$ can always be demonstrated by (finitely many) successive applications of clauses above. (minimality clause)

Which of the numbers $9, 10, 11, 12, 13$ are in $S$? Which are not?

# CS1231S Chapter 9

# Functions




## 9.1 Basics

**Definition 7.2.1** (again)**.** Let $A, B$ be sets. A *function* or a *map* from $A$ to $B$ is an assignment to each element of $A$ exactly one element of $B$. We write $f\colon A \to B$ for "$f$ is a function from $A$ to $B$". Suppose $f\colon A \to B$.

(1) Let $x \in A$. Then $f(x)$ denotes the element of $B$ that $f$ assigns $x$ to. We call $f(x)$ the *image* of $x$ under $f$. If $y = f(x)$, then we say that $f$ *maps* $x$ *to* $y$, and we may write $f\colon x \mapsto y$.

(2) Here $A$ is called the *domain* of $f$, and $B$ is called the *codomain* of $f$.

**Remark 9.1.1.** (1) A sequence $a_0, a_1, a_2, \ldots$ can be represented by the function $a$ whose domain is $\mathbb{Z}_{\geqslant 0}$ that satisfies $a(n) = a_n$ for every $n \in \mathbb{Z}_{\geqslant 0}$.

(2) In this sense, any function whose domain is $\mathbb{Z}_{\geqslant m}$ for some $m \in \mathbb{Z}$ represents a sequence.

**Example 9.1.2.** One can represent the Fibonacci sequence $F_0, F_1, F_2, \ldots$ by the unique function $F\colon \mathbb{Z}_{\geqslant 0} \to \mathbb{Z}_{\geqslant 0}$ that satisfies, for each $n \in \mathbb{Z}_{\geqslant 0}$,

$$F(0) = 0 \quad \text{and} \quad F(1) = 1 \quad \text{and} \quad F(n+2) = F(n+1) + F(n).$$

Such an $F$ exists and is unique, essentially by Proposition 8.3.4.

**Definition 9.1.3.** Let $A$ be a set. A *string* or a *word* over $A$ is an expression of the form

$$a_0 a_1 \ldots a_{\ell-1}$$

where $\ell \in \mathbb{Z}_{\geqslant 0}$ and $a_0, a_1, \ldots, a_{\ell-1} \in A$. Here $\ell$ is called the *length* of the string. Let $A^*$ denote the set of all strings over $A$. The *empty string*, denoted $\varepsilon$, is the string of length 0.

**Example 9.1.4.** Let $A = \{\mathrm{s}, \mathrm{u}\}$. The following are strings over $A$:

$$A^* = \{\ \mathrm{s},\ \mathrm{ssuu},\ \mathrm{sususususu},\ \mathrm{uuuuuuuu},\ \ldots\ \}$$

Their lengths are respectively 1, 4, 8, and 7.

**Remark 9.1.5.** Let $A$ be a set.

(1) One can represent a string $a_0 a_1 \ldots a_{\ell-1}$ over $A$ by the function $a\colon \{0, 1, \ldots, \ell-1\} \to A$ satisfying $a(n) = a_n$ for all $n \in \{0, 1, \ldots, \ell-1\}$.

(2) Every function $a\colon \{m, m+1, \ldots, m+\ell-1\} \to A$, where $m \in \mathbb{Z}$ and $\ell \in \mathbb{Z}_{\geqslant 0}$, represents a string of length $\ell$ over $A$, namely $a(m)\, a(m+1)\, \ldots\, a(m+\ell-1)$.

**Definition 9.1.6.** Two functions $f\colon A \to B$ and $g\colon C \to D$ are *equal* if

(1) $A = C$ and $B = D$; and

(2) $f(x) = g(x)$ for all $x \in A$.

In this case, we write $f = g$.

**Example 9.1.7.** Let $f\colon \{0,2\} \to \mathbb{Z}$ and $g\colon \{0,2\} \to \mathbb{Z}$ defined by setting, for all $x \in \{0,2\}$,

$$f(x) = 2x \quad \text{and} \quad g(x) = x^2.$$

Then $f = g$ because their domains are the same, their codomains are the same, and $f(x) = g(x)$ for every $x \in \{0,2\}$.

**Example 9.1.8.** Let $f\colon \mathbb{Z} \to \mathbb{Z}$ and $g\colon \mathbb{Z} \to \mathbb{Q}$ defined by setting, for all $x \in \mathbb{Z}$,

$$f(x) = x^3 = g(x).$$

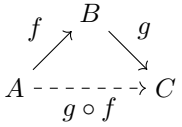
Then $f \neq g$ because they have different codomains.

## 9.2 Composition

**Definition 9.2.1.** Let $f\colon A \to B$ and $g\colon B \to C$. Then $g \circ f\colon A \to C$ such that for every $x \in A$,

$$(g \circ f)(x) = g(f(x)).$$

We read $g \circ f$ as "$g$ composed with $f$", or "$g$ circle $f$".



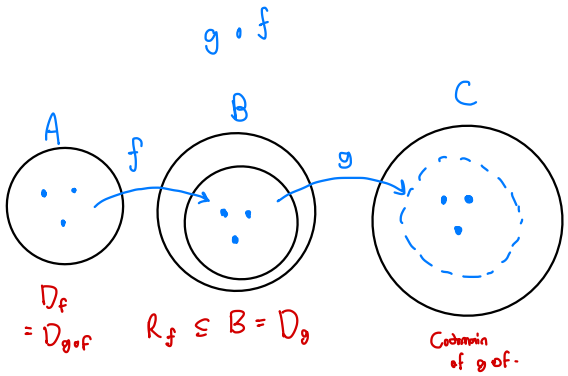




Figure 9.1: Function composition

**Note 9.2.2.** For $g \circ f$ to be defined, the codomain of $f$ must equal the domain of $g$.

**Example 9.2.3.** Let $f\colon A \to B$.

(1) $f \circ \mathrm{id}_A = f$ because

- the domain of $f \circ \mathrm{id}_A$ and the domain of $f$ are both $A$;
- the codomain of $f \circ \mathrm{id}_A$ and the codomain of $f$ are both $B$; and
- $(f \circ \mathrm{id}_A)(x) = f(\mathrm{id}_A(x)) = f(x)$ for all $x \in A$.

(2) $\mathrm{id}_B \circ f = f$ because

- the domain of $\mathrm{id}_B \circ f$ and the domain of $f$ are both $A$;
- the codomain of $\mathrm{id}_B \circ f$ and the codomain of $f$ are both $B$;
- $(\mathrm{id}_B \circ f)(x) = \mathrm{id}_B(f(x)) = f(x)$ for all $x \in A$.

**Question 9.2.4.** Which of the following define a function $f\colon \mathbb{Z} \to \mathbb{Z}$ that satisfies $f \circ f = f$? 9a

(1) $f(x) = 1231$ for all $x \in \mathbb{Z}$.

(2) $f(x) = x$ for all $x \in \mathbb{Z}$.

(3) $f(x) = -x$ for all $x \in \mathbb{Z}$.

(4) $f(x) = 3x + 1$ for all $x \in \mathbb{Z}$.

(5) $f(x) = x^2$ for all $x \in \mathbb{Z}$.

**Example 9.2.5.** Let $f, g\colon \mathbb{Z} \to \mathbb{Z}$ such that for every $x \in \mathbb{Z}$,

$$f(x) = 3x \quad \text{and} \quad g(x) = x + 1.$$

Then for every $x \in \mathbb{Z}$,

$$(g \circ f)(x) = g(f(x)) = g(3x) = 3x + 1 \quad \text{and} \quad (f \circ g)(x) = f(g(x)) = f(x + 1) = 3(x + 1).$$

Note $(g \circ f)(0) = 1 \neq 3 = (f \circ g)(0)$.

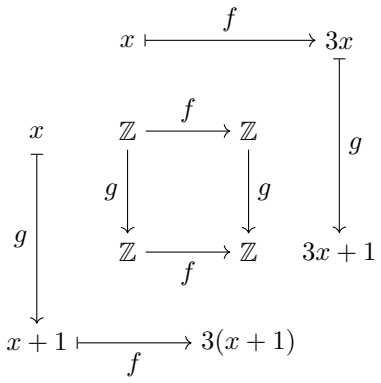



Figure 9.2: The two paths from the top left to the bottom right are not the same

**Theorem 9.2.6** (associativity of function composition)**.** Let $f\colon A \to B$ and $g\colon B \to C$ and $h\colon C \to D$. Then

$$(h \circ g) \circ f = h \circ (g \circ f).$$

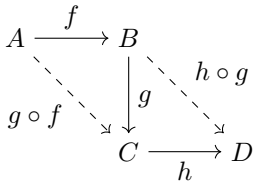


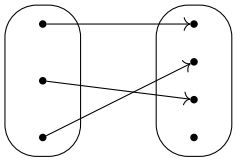

Figure 9.3: All paths from $A$ to $D$ are the same

**Proof.** 1. The domains of $(h \circ g) \circ f$ and $h \circ (g \circ f)$ are both $A$.
2. The codomains of $(h \circ g) \circ f$ and $h \circ (g \circ f)$ are both $D$.
3. For every $x \in A$,

$$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x))) = h((g \circ f)(x)) = (h \circ (g \circ f))(x). \qquad \square$$

## 9.3 Inverse

**Arrow diagrams.**



The figure above represents a function in the following sense.

- The dots on the left denote the elements of the domain.
- The dots on the right denote the elements of the codomain.
- An arrow from a left dot to a right dot indicates that the left dot is assigned the right dot.

Since every dot on the left is joined to exactly one dot on the right in the figure above, this function is well defined.

**Definition 9.3.1.** Let $f: A \to B$.

(1) If $X \subseteq A$, then let $f(X) = \{f(x) : x \in X\}$.

(2) If $Y \subseteq B$, then let $f^{-1}(Y) = \{x \in A : f(x) \in Y\}$.

We call $f(X)$ the *(setwise) image* of $X$, and $f^{-1}(Y)$ the *(setwise) preimage* of $Y$ under $f$.

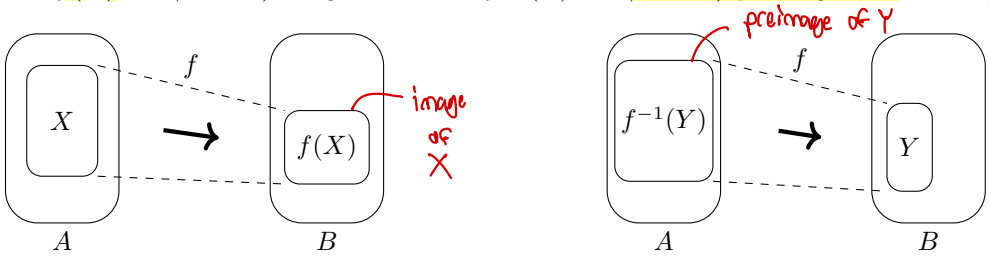
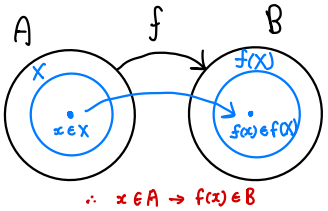



Figure 9.4: Setwise image and setwise preimage

**Example 9.3.2.** Define $g: \mathbb{Z} \to \mathbb{Z}$ by setting $g(x) = x^2$ for every $x \in \mathbb{Z}$.

(1) If $X = \{-1, 0, 1\}$, then $g(X) = \{g(-1), g(0), g(1)\} = \{1, 0, 1\} = \{0, 1\}$.

(2) If $Y = \{0, 1, 2\}$, then $g^{-1}(Y) = \{0, -1, 1\}$.




**Note 9.3.3.** Let $f: A \to B$.

(1) If $X \subseteq A$, then $f(X) = \{f(x) : x \in X\}$, which is a set. If $x \in A$, then $f(x) \in B$.

(2) If $Y \subseteq B$, then $f^{-1}(Y) = \{x \in A : f(x) \in Y\}$, which exists even when the inverse function $f^{-1}$ does not. If $y \in B$ and $f^{-1}$ exists, then $f^{-1}(y) \in A$.

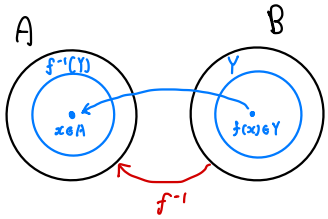
reverse mapping.

eg. not bijective.

The inverse of a function will be defined in Definition 9.3.14.

**Question 9.3.4.** As in Example 9.3.2, define $g: \mathbb{Z} \to \mathbb{Z}$ by setting $g(x) = x^2$ for every $x \in \mathbb{Z}$. 9b
Which of the following are true statements?

- $g(0) = 0$.
- $g(0) = \{0\}$.

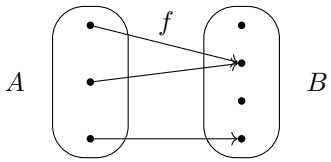



$Y \neq f(X)$

If $y \in B$ and $f^{-1}$ exist, then $f^{-1}(y) \in A$

- $g(\{0\}) = 0$.
- $g(\{0\}) = \{0\}$.

**Note 9.3.5.** In general, we cannot make $f^{-1}$ operate on elements instead of subsets.




**Definition 9.3.6.** Let $f\colon A \to B$.

(1) $f$ is *surjective* or *onto* if

$$\forall y \in B \;\; \exists x \in A \;\; (y = f(x)).$$

A *surjection* is a surjective function. Every elem in codomain have one elem in domain that maps to it $|A| \geq |B|$ (note: function can have :> but not •<:).

(2) $f$ is *injective* or *one-to-one* if

$$\forall x_1, x_2 \in A \;\; (f(x_1) = f(x_2) \Rightarrow x_1 = x_2).$$

An *injection* is an injective function.

(3) $f$ is *bijective* if it is both surjective and injective, i.e.,

$$\forall y \in B \;\; \exists! x \in A \;\; (y = f(x)).$$

A *bijection* is a bijective function.

**Example 9.3.7.** The function $f\colon \mathbb{Q} \to \mathbb{Q}$, defined by setting $f(x) = 3x + 1$ for all $x \in \mathbb{Q}$, is surjective.

**Proof.** 1. Take any $y \in \mathbb{Q}$.
2. Let $x = (y - 1)/3$.
3. Then $x \in \mathbb{Q}$ and $f(x) = 3x + 1 = y$. □

**Remark 9.3.8.** A function $f\colon A \to B$ is *not* surjective if and only if

$$\exists y \in B \;\; \forall x \in A \;\; (y \neq f(x)).$$

**Example 9.3.9.** As in Example 9.3.2, define $g\colon \mathbb{Z} \to \mathbb{Z}$ by setting $g(x) = x^2$ for every $x \in \mathbb{Z}$. Then $g$ is not surjective.

**Proof.** 1. Note $g(x) = x^2 \geqslant 0 > -1$ for all $x \in \mathbb{Z}$.
2. So $g(x) \neq -1$ for all $x \in \mathbb{Z}$, although $-1 \in \mathbb{Z}$. □

**Example 9.3.10.** As in Example 9.3.7, define $f\colon \mathbb{Q} \to \mathbb{Q}$ by setting $f(x) = 3x + 1$ for all $x \in \mathbb{Q}$. Then $f$ is injective.

**Proof.** 1. Let $x_1, x_2 \in \mathbb{Q}$ such that $f(x_1) = f(x_2)$.
2. Then $3x_1 + 1 = 3x_2 + 1$.
3. So $x_1 = x_2$. □

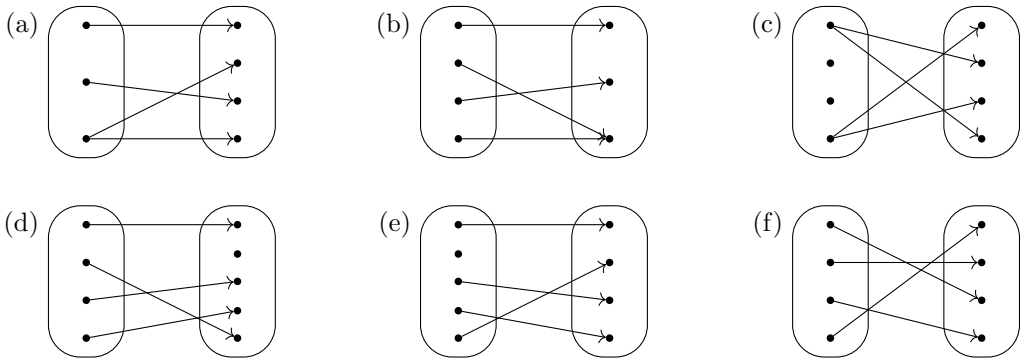
**Remark 9.3.11.** A function $f\colon A \to B$ is *not* injective if and only if

$$\exists x_1, x_2 \in A \;\; (f(x_1) = f(x_2) \wedge x_1 \neq x_2).$$

**Example 9.3.12.** As in Example 9.3.2, define $g\colon \mathbb{Z} \to \mathbb{Z}$ by setting $g(x) = x^2$ for every $x \in \mathbb{Z}$. Then $g$ is not injective.

**Proof.** Note $g(1) = 1^2 = 1 = (-1)^2 = g(-1)$, although $1 \neq -1$. □

**Question 9.3.13.** Which of the arrow diagrams below represent a function from the LHS set to the RHS set? Amongst those that represent a function, which ones represent injections, which ones represent surjections, and which ones represent bijections? 9c




**Definition 9.3.14.** Let $f\colon A \to B$. Then $g\colon B \to A$ is an *inverse* of $f$ if

$$\forall x \in A \;\; \forall y \in B \;\; \big(y = f(x) \quad \Leftrightarrow \quad x = g(y)\big).$$

bijection.

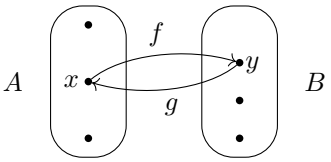



Figure 9.5: An inverse of a function

**Example 9.3.15.** As in Example 9.3.10, define $f\colon \mathbb{Q} \to \mathbb{Q}$ by setting $f(x) = 3x + 1$ for all $x \in \mathbb{Q}$. Note that for all $x, y \in \mathbb{Q}$,

$$y = 3x + 1 \quad \Leftrightarrow \quad x = (y - 1)/3.$$

Let $g\colon \mathbb{Q} \to \mathbb{Q}$ such that $g(y) = (y - 1)/3$ for all $y \in \mathbb{Q}$. Then the equivalence above tells us

$$\forall x, y \in \mathbb{Q} \;\; (y = f(x) \Leftrightarrow x = g(y)).$$

So $g$ is an inverse of $f$.

**Note 9.3.16.** We have no guarantee of a description of an inverse of a general function that is much different from what is given by the definitions.

**Proposition 9.3.17** (uniqueness of inverses)**.** If $g_1, g_2$ are inverses of $f\colon A \to B$, then $g_1 = g_2$.

**Proof.** 1. Note $g_1, g_2\colon B \to A$.
2. Since $g_1, g_2$ are inverses of $f$, for all $x \in A$ and all $y \in B$,

$$x = g_1(y) \quad \Leftrightarrow \quad y = f(x) \quad \Leftrightarrow \quad x = g_2(y).$$

3. So $g_1 = g_2$. □

**Definition 9.3.18.** The inverse of a function $f$ is denoted $f^{-1}$.

**Theorem 9.3.19.** A function $f\colon A \to B$ is bijective if and only if it has an inverse.

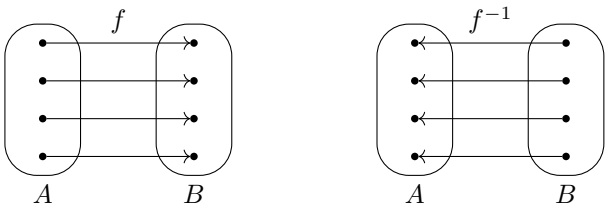



Figure 9.6: A bijective function and its inverse

**Proof.** 1. ("If")
- 1.1. Suppose $f$ has an inverse, say $g\colon B \to A$.
- 1.2. We first show injectivity.
  - 1.2.1. Let $x_1, x_2 \in A$ such that $f(x_1) = f(x_2)$.
  - 1.2.2. Define $y = f(x_1) = f(x_2)$.
  - 1.2.3. Then $x_1 = g(y)$ and $x_2 = g(y)$ as $g$ is an inverse of $f$.
  - 1.2.4. Thus $x_1 = x_2$.
- 1.3. Next we show surjectivity.
  - 1.3.1. Let $y \in B$.
  - 1.3.2. Define $x = g(y)$.
  - 1.3.3. Then $y = f(x)$ as $g$ is an inverse of $f$.

2. ("Only if")
- 2.1. Suppose $f$ is bijective.
- 2.2. Then $\forall y \in B \;\; \exists! x \in A \;\; (y = f(x))$.
- 2.3. Define the function $g\colon B \to A$ by setting $g(y)$ to be the unique $x \in A$ such that $y = f(x)$ for all $y \in B$.
- 2.4. This $g$ is well defined and is an inverse of $f$ by the definition of inverse functions. □

# CS1231S Chapter 10

# Cardinality

## 10.1 Pigeonhole Principles

**Theorem 10.1.1** (Pigeonhole Principle)**.** Let $A$ and $B$ be finite sets. If there is an injection $f\colon A \to B$, then $|A| \leqslant |B|$. injection ⇒ $|A| \leq |B|$

**Proof.** 1. Note that $A$ is finite. Suppose $A = \{a_1, a_2, \ldots, a_m\}$, where $m = |A|$.
2. The injectivity of $f$ tells us that, if $a_i \neq a_j$, then $f(a_i) \neq f(a_j)$.
3. So $f(a_1), f(a_2), \ldots, f(a_m)$ are $m$ different elements of $B$.
4. This shows $|B| \geqslant m = |A|$. □

**Theorem 10.1.2** (Dual Pigeonhole Principle)**.** Let $A$ and $B$ be finite sets. If there is a surjection $f\colon A \to B$, then $|A| \geqslant |B|$. surjection ⇒ $|A| \geq |B|$

**Proof.** 1. Note that $B$ is finite. Suppose $B = \{b_1, b_2, \ldots, b_n\}$, where $n = |B|$.
2. For each $b_i$, use the surjectivity of $f$ to find $a_i \in A$ such that $f(a_i) = b_i$.
3. If $b_i \neq b_j$, then $f(a_i) \neq f(a_j)$, and so $a_i \neq a_j$ because $f$ is a function.
4. So $a_1, a_2, \ldots, a_n$ are $n$ different elements of $A$.
5. This shows $|A| \geqslant n = |B|$. □

**Theorem 10.1.3.** Let $A$ and $B$ be finite sets. Then there is a bijection $A \to B$ if and only if $|A| = |B|$. bijection ⇒ $|A| = |B|$.

**Proof.** 1. ("Only if") This follows directly from Theorem 10.1.1 and Theorem 10.1.2.
2. ("If")
   2.1. Suppose $|A| = |B| = n$.
   2.2. Let $a_1, a_2, \ldots, a_n$ be the $n$ elements of $A$, and $b_1, b_2, \ldots, b_n$ be the $n$ elements of $B$.
   2.3. Note that the list $a_1, a_2, \ldots, a_n$ cannot have repetition because $|A| = n$.
   2.4. Similarly, the list $b_1, b_2, \ldots, b_n$ has no repetition.
   2.5. Define functions $f\colon A \to B$ and $g\colon B \to A$ by setting $f(a_i) = b_i$ and $g(b_i) = a_i$ for all $i \in \{1, 2, \ldots, n\}$.
   2.6. As the lists $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$ have no repetition, the functions $f$ and $g$ are well defined.
   2.7. Observe that $g = f^{-1}$ by the definition of inverses.
   2.8. So $f$ is a bijection $A \to B$ by Theorem 9.3.19. □

**Exercise 10.1.4.** Prove the converse to Theorem 10.1.1. Prove also the converse to Theorem 10.1.2 when $B \neq \varnothing$. 10a

## 10.2 Same cardinality

**Definition 10.2.1** (Cantor)**.** A set $A$ is said to have the *same cardinality* as a set $B$ if there is a bijection $A \to B$. In this case, we write $|A| = |B|$.

iff

**Note 10.2.2.** We defined what $|A| = |B|$ means without defining what $|A|$ and $|B|$ mean.

**Proposition 10.2.3.** Let $A, B, C$ be sets. Equivalent Relation.

(1) $|A| = |A|$. (reflexivity)

(2) If $|A| = |B|$, then $|B| = |A|$. (symmetry)

(3) If $|A| = |B|$ and $|B| = |C|$, then $|A| = |C|$. (transitivity)

**Proof.** 1. (Reflexivity.) It suffices to show that $\mathrm{id}_A$ is a bijection $A \to A$.
   1.1. $\mathrm{id}_A$ is injective because if $x_1, x_2 \in A$ such that $\mathrm{id}_A(x_1) = \mathrm{id}_A(x_2)$, then $x_1 = x_2$.
   1.2. $\mathrm{id}_A$ is surjective because given any $x \in A$, we have $\mathrm{id}_A(x) = x$.
2. (Symmetry.)
   2.1. Suppose $|A| = |B|$.
   2.2. Use the definition of same-cardinality to find a bijection $f\colon A \to B$.
   2.3. Then Theorem 9.3.19 gives us an inverse of $f$; call it $g$.
   2.4. By the definition of inverses, for all $x \in A$ and all $y \in B$,

$$y = f(x) \quad \Leftrightarrow \quad x = g(y).$$

   2.5. This tells us that $f$ is an inverse of $g$ in view the definition of inverses.
   2.6. Thus $g$ is a bijection $B \to A$ by Theorem 9.3.19.
   2.7. This shows $|B| = |A|$.
3. (Transitivity.)
   3.1. Suppose $|A| = |B|$ and $|B| = |C|$.
   3.2. Use the definition of same-cardinality to find a bijection $f\colon A \to B$ and a bijection $g\colon B \to C$.
   3.3. Then Tutorial 7 Question 8 tells us $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.
   3.4. In particular, this says $g \circ f$ has an inverse.
   3.5. So $g \circ f$ is a bijection $A \to C$ by Theorem 9.3.19.
   3.6. Hence $|A| = |C|$. □

## 10.3 Countability

**Definition 10.3.1** (Cantor)**.** A set is *countable* if it is finite or it has the same cardinality as $\mathbb{Z}_{\geqslant 0}$. bijection to $\mathbb{N}$

**Note 10.3.2.** Some authors allow only infinite sets to be countable.

**Example 10.3.3.** (1) $|\mathbb{Z}_{\geqslant 0}| = |\mathbb{Z}_{\geqslant 0} \setminus \{0\}|$ because the function $f\colon \mathbb{Z}_{\geqslant 0} \to \mathbb{Z}_{\geqslant 0} \setminus \{0\}$ satisfying $f(x) = x + 1$ for all $x \in \mathbb{Z}_{\geqslant 0}$ is a bijection. So $\mathbb{Z}_{\geqslant 0} \setminus \{0\} = \{1, 2, 3, \dots\}$ is countable.

(2) $|\mathbb{Z}_{\geqslant 0}| = |\mathbb{Z}_{\geqslant 0} \setminus \{1, 3, 5, \dots\}|$ because the function $g\colon \mathbb{Z}_{\geqslant 0} \to \mathbb{Z}_{\geqslant 0} \setminus \{1, 3, 5, \dots\}$ satisfying $g(x) = 2x$ for all $x \in \mathbb{Z}_{\geqslant 0}$ is a bijection. So $\mathbb{Z}_{\geqslant 0} \setminus \{1, 3, 5, \dots\} = \{0, 2, 4, \dots\}$ is countable.

**Note 10.3.4.** An infinite set $B$ is countable if and only if

there is a sequence $b_0, b_1, b_2, \dots \in B$ in which every element of $B$ appears exactly once.

aka bijection

**Proof.** 1. ("If")
   1.1. Let $b_0, b_1, b_2, \dots$ be a sequences of elements of $B$ in which every element of $B$ appears exactly once.
   1.2. Define $f\colon \mathbb{Z}_{\geqslant 0} \to B$ by setting $f(i) = b_i$ for each $i \in \mathbb{Z}_{\geqslant 0}$.
   1.3. Then $f$ is well defined because $b_0, b_1, b_2, \dots \in B$.

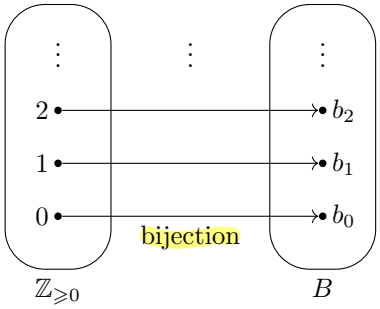



Figure 10.1: A countable infinite set $B$

1.4. (Surjectivity)
  1.4.1. Let $b \in B$.
  1.4.2. Then $b = b_i$ for some $i \in \mathbb{Z}_{\geqslant 0}$ because every element of $B$ appears in $b_0, b_1, b_2, \ldots$.
  1.4.3. So $b = f(i)$ for some $i \in \mathbb{Z}_{\geqslant 0}$ by the definition of $f$.
1.5. (Injectivity)
  1.5.1. Let $i, j \in \mathbb{Z}_{\geqslant 0}$ such that $f(i) = f(j)$.
  1.5.2. Then $b_i = b_j$ by the definition of $f$.
  1.5.3. Thus $i = j$ because every element of $B$ appears in $b_0, b_1, b_2, \ldots$ at most once.

2. ("Only if")
  2.1. Let $f$ be a bijection $\mathbb{Z}_{\geqslant 0} \to B$.
  2.2. Define $b_0, b_1, b_2, \ldots$ to be $f(0), f(1), f(2), \ldots$ respectively.
  2.3. Then $b_0, b_1, b_2, \cdots \in B$ because the codomain of $f$ is $B$.
  2.4. For every $b \in B$, there is $i \in \mathbb{Z}_{\geqslant 0}$ such that $b = f(i) = b_i$ by the surjectivity of $f$.
  2.5. So every element of $B$ appears at least once in $b_0, b_1, b_2, \ldots$.
  2.6. Whenever $i, j \in \mathbb{Z}_{\geqslant 0}$ such that $b_i = b_j$, then $f(i) = f(j)$ and so $i = j$ by the injectivity of $f$.
  2.7. In particular, every element of $B$ appears at most once in $b_0, b_1, b_2, \ldots$.
  2.8. Hence every element of $B$ appears exactly once in $b_0, b_1, b_2, \ldots$. □

**Lemma 10.3.5.** An infinite set $B$ is countable if and only if

there is a sequence $c_0, c_1, c_2, \ldots$ in which every element of $B$ appears.

**Proof.** 1. ("Only if") This follows directly from Note 10.3.4.

2. ("If")
  2.1. Let $c_0, c_1, c_2, \ldots$ be a sequence in which every element of $B$ appears.
  2.2. Remove those terms in the sequence that are not in $B$.
  2.3. If an element of $B$ appears more than once, then remove all but the first appearance.
  2.4. The result is a sequence in which every element of $B$ appears exactly once.
  2.5. So $B$ is countable. □

**Proposition 10.3.6.** Any subset $A$ of a countable set $B$ is countable. $A \subseteq B$, $A$ and $B$ are both countable.

**Proof.** 1. If $A$ is finite, then $A$ is countable by definition.

2. So suppose $A$ is infinite.
  2.1. Then $B$ is infinite too as $A \subseteq B$.
  2.2. Use the countability of $B$ to find a sequence $b_0, b_1, b_2, \ldots$ in which every element of $B$ appears exactly once.
  2.3. This is a sequence in which every element of $A$ appears.
  2.4. So $A$ is countable by Lemma 10.3.5. □

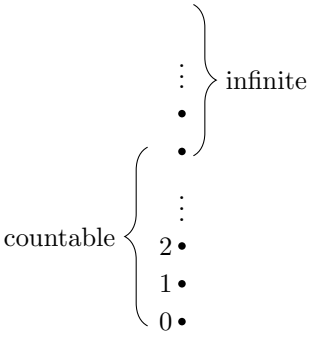



Figure 10.2: The smallest cardinalities

**Proposition 10.3.7.** Every infinite set $B$ has a countable infinite subset.

**Proof.** 1. Keep choosing elements $b_0, b_1, b_2, \dots$ from $B$. When we choose $b_n$, where $n \in \mathbb{Z}_{\geqslant 0}$, we can always make sure $b_n \neq b_i$ for any $i < n$, because otherwise $B$ is equal to the finite set $\{b_0, b_1, \dots, b_{n-1}\}$, which is a contradiction.
2. The result is a countable infinite set $\{b_0, b_1, b_2, \dots\} \subseteq B$. □

## 10.4 Set operations

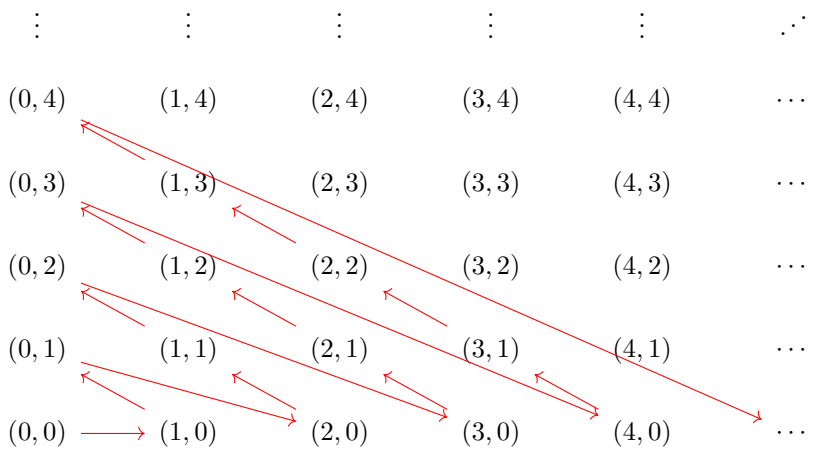
**Proposition 10.4.1.** Let $A, B$ be countable infinite sets. Then $A \cup B$ is countable.

$A \cup B$ ⇒ countable if $A$ & $B$ countable

**Proof.** 1. Apply Lemma 10.3.5 to find a sequence $a_0, a_1, a_2, \dots$ in which every element of $A$ appears.
2. Apply Lemma 10.3.5 to find a sequence $b_0, b_1, b_2, \dots$ in which every element of $B$ appears.
3. Then $a_0, b_0, a_1, b_1, a_2, b_2, \dots$ is a sequence in which every element of $A \cup B$ appears.
4. So $A \cup B$ is countable by Lemma 10.3.5. □

**Theorem 10.4.2** (Cantor 1877)**.** $\mathbb{Z}_{\geqslant 0} \times \mathbb{Z}_{\geqslant 0}$ is countable.

**Proof sketch.**




The figure above describes a sequence

$$(0,0), (1,0), (0,1), (2,0), (1,1), (0,2), (3,0), (2,1), (1,2), (0,3), (4,0), (3,1), (2,2), (1,3), (0,4), \dots$$

in which every element of $\mathbb{Z}_{\geqslant 0} \times \mathbb{Z}_{\geqslant 0}$ appears. So $\mathbb{Z}_{\geqslant 0} \times \mathbb{Z}_{\geqslant 0}$ is countable by Lemma 10.3.5. □

**Theorem 10.4.3** (Cantor 1891)**.** Let $A$ be a countable infinite set. Then $\mathcal{P}(A)$ is not countable.

**Proof.** Given any sequence of elements of $\mathcal{P}(A)$, we will produce an element of $\mathcal{P}(A)$ that does not appear in it. This will show that no sequence of elements of $\mathcal{P}(A)$ contains all the elements of $\mathcal{P}(A)$, and thus $\mathcal{P}(A)$ is uncountable by Note 10.3.4.

We organize all these into a proof by contradiction.

1. Suppose $\mathcal{P}(A)$ is countable.
2. We know $\mathcal{P}(A)$ is infinite because $A$ is infinite and $\{a\} \in \mathcal{P}(A)$ for every $a \in A$.
3. Use the countability of $\mathcal{P}(A)$ to find a sequence $B_0, B_1, B_2, \ldots \in \mathcal{P}(A)$ in which every element of $\mathcal{P}(A)$ appears exactly once.
4. Use the countability of $A$ to find a sequence $a_0, a_1, a_2, \ldots \in A$ in which every element of $A$ appears exactly once.
5. Define $B = \{a_i : a_i \notin B_i\}$.
6. Note that $B \subseteq A$ since $a_0, a_1, a_2, \ldots \in A$.
7. 7.1. Let $i \in \mathbb{Z}_{\geqslant 0}$.
   7.2. If $a_i \notin B_i$, then $a_i \in B$ by the definition of $B$.
   7.3. if $a_i \in B_i$, then $a_i \notin B$ by the definition of $B$ because no $j \neq i$ makes $a_j = a_i$ by the choice of $a_0, a_1, a_2, \ldots$.
   7.4. In either case, we know $B \neq B_i$.
8. This contradicts line 3 that every element of $\mathcal{P}(A)$ appears in $B_0, B_1, B_2, \ldots$. □

| | $a_0$ | $a_1$ | $a_2$ | $a_3$ | $a_4$ | $\ldots$ |
|---|---|---|---|---|---|---|
| $B_0$ | $\boxed{\notin}$ | $\in$ | $\notin$ | $\notin$ | $\notin$ | $\ldots$ |
| $B_1$ | $\in$ | $\boxed{\notin}$ | $\in$ | $\notin$ | $\in$ | $\ldots$ |
| $B_2$ | $\notin$ | $\in$ | $\boxed{\in}$ | $\notin$ | $\in$ | $\ldots$ |
| $B_3$ | $\notin$ | $\notin$ | $\in$ | $\boxed{\notin}$ | $\notin$ | $\ldots$ |
| $B_4$ | $\in$ | $\notin$ | $\in$ | $\in$ | $\boxed{\notin}$ | $\ldots$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\ddots$ |
| new $B$ | $\in$ | $\in$ | $\notin$ | $\in$ | $\in$ | $\ldots$ |

Figure 10.3: Illustration of Cantor's diagonal argument

**Exercise 10.4.4.** Which of the following is/are countable? Justify your answer. 10b

(1) $\mathbb{Z}$. yes

(2) $\mathbb{Q}$. yes

(3) $\mathbb{R}$. no

(4) $\mathbb{C}$. no

(5) The set of all finite sets of integers. no

(6) The set of all strings over $\{s, u\}$. yes.

(7) The set of all (infinite) sequences over $\{0, 1\}$. no (Set of all function $\mathbb{Z}_{\geq 0} \to \{0,1\}$).

(8) The set of all functions $A \to B$ where $A, B$ are finite sets of integers. yes.

(9) The set of all computer programs. yes.
↓
string over $\{0,1\}$

## Tutorial questions 8

1. Let $n \in \mathbb{Z}^+$. Recall from Definition 7.1.4 that $\mathbb{Z}_n$ denotes the quotient of $\mathbb{Z}$ by the congruence-mod-$n$ relation. Let $[a], [b] \in \mathbb{Z}_n$. Prove that $[a]$ has the same cardinality as $[b]$. (Hint: You may find Example 6.4.3 helpful.)

2. Let $B$ be a countable infinite set and $C$ be a finite set. Show that $B \cup C$ is countable.

3. Let $B$ be a (not necessarily countable) infinite set and $C$ be a finite set. Define a bijection $B \cup C \to B$.

4. Prove that a set $B$ is infinite if and only if there is $A \subsetneq B$ such that $|A| = |B|$.

5. Let $S_i$ be a countable infinite set for each $i \in \mathbb{Z}_{\geqslant 0}$. Prove that $\bigcup_{i \in \mathbb{Z}_{\geqslant 0}} S_i$ is countable.

6. Let $S_i$ be a countable (not necessarily infinite) set for each $i \in \mathbb{Z}_{\geqslant 0}$. Prove that $\bigcup_{i \in \mathbb{Z}_{\geqslant 0}} S_i$ is countable.

7. For each $n \in \mathbb{Z}_{\geqslant 0}$, define $F_n = \{X \in \mathcal{P}(\mathbb{Z}_{\geqslant 0}) : |X| = n\}$. Let $F = \bigcup_{n \in \mathbb{Z}_{\geqslant 0}} F_n$.

   (a) Prove that $F_n$ is countable for every $n \in \mathbb{Z}_{\geqslant 1}$ by induction on $n$.

   (b) Deduce that $F$ is countable.

8. In the answer to Exercise 10.4.4 in the notes, it is proved that $\mathbb{Q}_{\geqslant 0}$ is countable. Use this fact to show that $\mathbb{Q}$ is countable.

9. Let $A = \{x \in \mathbb{R} : 0 \leqslant x < 1\}$. Using a diagonal argument, or otherwise, prove that $A$ is uncountable.

   You may use without proof the fact that the elements of $A$ are precisely those real numbers that have a decimal representation

   $$0.d_0d_1d_2d_3d_4\ldots$$

   without a tail of 9's; moreover, such a representation is unique.

10. Prove that $\mathbb{R}$ and $\mathbb{C}$ are uncountable.

Tutorial 1:

9. Recall the definitions of even and odd integers in Lecture #1 slide 27:

> If $n$ is an integer, then
> $n$ is even if and only if $\exists k \in \mathbb{Z}$ s.t. $n = 2k$;
> $n$ is odd if and only if $\exists k \in \mathbb{Z}$ s.t. $n = 2k + 1$.

Prove the following:

The product of any two odd integers is an odd integer.

# Summary

## 9.1 Introduction

### Definitions

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

### Notation

For a finite set $A$, $|A|$ denotes the number of elements in $A$.

### Equally Likely Probability Formula

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

$$P(E) = \frac{\text{The number of outcomes in } E}{\text{The total number of outcomes in } S} = \frac{|E|}{|S|}$$

### Theorem 9.1.1 The Number of Elements in a List

If $m$ and $n$ are integers and $m \le n$, then there are $n - m + 1$ integers from $m$ to $n$ inclusive.

# Summary



## Theorem 9.2.1 The Multiplication/Product Rule

If an operation consists of $k$ steps and

the first step can be performed in $n_1$ ways,

the second step can be performed in $n_2$ ways

(regardless of how the first step was performed),

:

the $k^{th}$ step can be performed in $n_k$ ways

(regardless of how the preceding steps were performed),

Then the entire operation can be performed in

$$n_1 \times n_2 \times n_3 \times \ldots \times n_k \text{ ways.}$$

# Summary



## Theorem 9.2.2 Permutations

The number of permutations of a set with $n$ ($n \geq 1$) elements is $\boldsymbol{n!}$

## Definition

An ***r*-permutation** of a set of $n$ elements is an ordered selection of $r$ elements taken from the set.
The number of $r$-permutations of a set of $n$ elements is denoted $\boldsymbol{P(n, r)}$.

## Theorem 9.2.3 $r$-permutations from a set of $n$ elements

If $n$ and $r$ are integers and $1 \leq r \leq n$, then the number of $r$-permutations of a set of $n$ elements is given by the formula

$$P(n, r) = n(n-1)(n-2)\ldots(n-r+1)$$ first version

or, equivalently,

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

# Summary

## 9.3 Counting Elements of Disjoint Sets

### Theorem 9.3.1 The Addition/Sum Rule

Suppose a finite set $A$ equals the union of $k$ distinct mutually disjoint subsets $A_1, A_2, \ldots, A_k$. Then $|A| = |A_1| + |A_2| + \ldots + |A_k|$.

### Theorem 9.3.2 The Difference Rule

If $A$ is a finite set and $B \subseteq A$, then $|A \setminus B| = |A| - |B|$.

### Formula for the Probability of the Complement of an Event

If $S$ is a finite sample space and $A$ is an event in $S$, then $P(\bar{A}) = 1 - P(A)$.

### Theorem 9.3.3 The Inclusion/Exclusion Rule for 2 or 3 Sets

If $A$, $B$, and $C$ are any finite sets, then

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

and

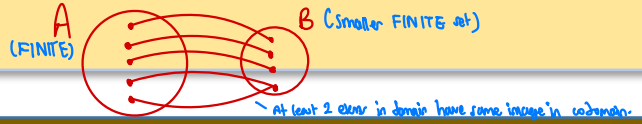
$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

# Summary



## Pigeonhole Principle (PHP)

A function from one finite set to a smaller finite set cannot be one-to-one:
There must be at least 2 elements in the domain that have the same image in the co-domain.




## Generalized Pigeonhole Principle

For any function $f$ from a finite set $X$ with $n$ elements to a finite set $Y$ with $m$ elements and for any positive integer $k$, if $k < n/m$, then
there is some $y \in Y$ such that $y$ is the image of at least $k + 1$ distinct elements of $X$.

## Generalized Pigeonhole Principle (Contrapositive Form)

For any function $f$ from a finite set $X$ with $n$ elements to a finite set $Y$ with $m$ elements and for any positive integer $k$,
if for each $y \in Y$, $f^{-1}(\{y\})$ has at most $k$ elements,
then $X$ has at most $km$ elements; in other words, $n \leq km$.

# Summary



## Definition: *r*-combination

Let $n$ and $r$ be non-negative integers with $r \leq n$.

An ***r*-combination** of a set of $n$ elements is a subset of $r$ of the $n$ elements.

$\binom{n}{r}$, read "$n$ choose $r$", denotes the number of subsets of size $r$ ($r$-combinations) that can be chosen from a set of $n$ elements.

Other symbols used are $C(n, r)$, ${}_nC_r$, $C_{n,r}$, or ${}^nC_r$.

## Theorem 9.5.1 Formula for $\binom{n}{r}$

The number of subsets of size $r$ (or $r$-combinations) that can be chosen from a set of $n$ elements, $\binom{n}{r}$, is given by the formula

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

or, equivalently,

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

where $n$ and $r$ are non-negative integers with $r \leq n$.

## Theorem 9.5.2 Permutations with sets of indistinguishable objects

Suppose a collection consists of $n$ objects of which

$n_1$ are of type 1 and are indistinguishable from each other
$n_2$ are of type 2 and are indistinguishable from each other
:
$n_k$ are of type $k$ and are indistinguishable from each other

and suppose that $n_1 + n_2 + \ldots + n_k = n$. Then the number of distinguishable permutations of the $n$ objects is

$$\binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\cdots\binom{n-n_1-n_2-\cdots-n_{k-1}}{n_k} = \frac{n!}{n_1!n_2!n_3!\cdots n_k!}$$

# Summary



## Definition: Multiset

An ***r*-combination with repetition allowed**, or **multiset of size *r***, chosen from a set *X* of *n* elements is an unordered selection of elements taken from *X* with repetition allowed.

If $X = \{x_1, x_2, \cdots, x_n\}$, we write an *r*-combination with repetition allowed as $[x_{i_1}, x_{i_2}, \cdots, x_{i_r}]$ where each $x_{i_j}$ is in *X* and some of the $x_{i_j}$ may equal each other.

## Theorem 9.6.1 Number of *r*-combinations with Repetition Allowed

The number of *r*-combination with repetition allowed (multisets of size *r*) that can be selected from a set of *n* elements is:

$$\binom{r+n-1}{r}$$

This equals the number of ways *r* objects can be selected from *n* categories of objects with repetitions allowed.

# Summary



## Which formula to use?

n: elements  k: no. of ways objects can be selected.

| | Order Matters | Order Does Not Matter |
|---|---|---|
| **Repetition Is Allowed** | $n^k$ | $\binom{k+n-1}{k}$ |
| **Repetition Is Not Allowed** | $P(n,k)$ | $\binom{n}{k}$ |

# Summary



## Theorem 9.7.1 Pascal's Formula

Let $n$ and $r$ be positive integers, $r \leq n$. Then

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$$

also
$\binom{n}{r} = \binom{n}{n-r}$
eg. $\binom{n}{n} = \binom{n}{0}$
$\binom{n}{1} = \binom{n}{n-1}$

## Theorem 9.7.2 Binomial Theorem

Given any real numbers $a$ and $b$ and any non-negative integer $n$,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \qquad \binom{n}{r} a^{n-r} b^r$$

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

## Theorem 6.3.1 Number of elements in a Power Set

If a set $X$ has $n$ ($n \geq 0$) elements, then $\wp(X)$ has $2^n$ elements.

# Summary



## Probability Axioms

Let $S$ be a sample space. A probability function $P$ from the set of all events in $S$ to the set of real numbers satisfies the following axioms: For all events $A$ and $B$ in $S$,

1. $0 \le P(A) \le 1$
2. $P(\varnothing) = 0$ and $P(S) = 1$
3. If $A$ and $B$ are disjoint ($A \cap B = \varnothing$), then $P(A \cup B) = P(A) + P(B)$

## Probability of the Complement of an Event

If $A$ is any event in a sample space $S$, then

$$P(\bar{A}) = 1 - P(A)$$

## Probability of a General Union of Two Events

If $A$ and $B$ are any events in a sample space $S$, then

$$P(A \cup B) = P(A) + P(B) - P(A \cap B).$$

# Summary



## Definition: Expected Value

Suppose the possible outcomes of an experiment, or random process, are real numbers $a_1, a_2, a_3, \cdots, a_n$ which occur with probabilities $p_1, p_2, p_3, \cdots, p_n$. The **expected value** of the process is

$$\sum_{k=1}^{n} a_k p_k = a_1 p_1 + a_2 p_2 + a_3 p_3 + \cdots + a_n p_n$$

## Linearity of Expectation

The expected value of the sum of random variables is equal to the sum of their individual expected values, regardless of whether they are independent. For random variables $X$ and $Y$,

$$E[X + Y] = E[X] + E[Y]$$

For random variables $X_1, X_2, \cdots, X_n$ and constants $c_1, c_2, \cdots, c_n$,

$$E\left[\sum_{i=1}^{n} c_i \cdot X_i\right] = \sum_{i=1}^{n} (c_i \cdot E[X_i])$$

# Summary



## Definition: Conditional Probability

Let $A$ and $B$ be events in a sample space $S$. If $P(A) \neq 0$, then the **conditional probability of $B$ given $A$**, denoted $P(B|A)$, is

$$P(B|A) = \frac{P(A \cap B)}{P(A)} \quad 9.9.1$$

$$P(A \cap B) = P(B|A) \cdot P(A) \quad 9.9.2$$

$$P(A) = \frac{P(A \cap B)}{P(B|A)} \quad 9.9.3$$

## Theorem 9.9.1 Bayes' Theorem

Suppose that a sample space $S$ is a union of mutually disjoint events $B_1, B_2, B_3, \ldots, B_n$. Suppose $A$ is an event in $S$, and suppose $A$ and all the $B_i$ have non-zero probabilities. If $k$ is an integer with $1 \leq k \leq n$, then

$$P(B_k|A) = \frac{P(A|B_k) \cdot P(B_k)}{P(A|B_1) \cdot P(B_1) + P(A|B_2) \cdot P(B_2) + \cdots + P(A|B_n) \cdot P(B_n)}$$

$P(A \cap B_k)$ $P(A \cap B_1)$

# Summary



## Definition: Independent Events

If $A$ and $B$ are events in a sample space $S$, then $A$ and $B$ are **independent**, if and only if,

$$P(A \cap B) = P(A) \cdot P(B)$$

## Definition: Pairwise Independent and Mutually Independent

Let $A$, $B$ and $C$ be events in a sample space $S$. $A$ , $B$ and $C$ are **pairwise independent**, if and only if, they satisfy conditions 1 – 3 below. They are **mutually independent** if, and only if, they satisfy all four conditions below.

1. $P(A \cap B) = P(A) \cdot P(B)$
2. $P(A \cap C) = P(A) \cdot P(C)$
3. $P(B \cap C) = P(B) \cdot P(C)$
4. $P(A \cap B \cap C) = P(A) \cdot P(B) \cdot P(C)$

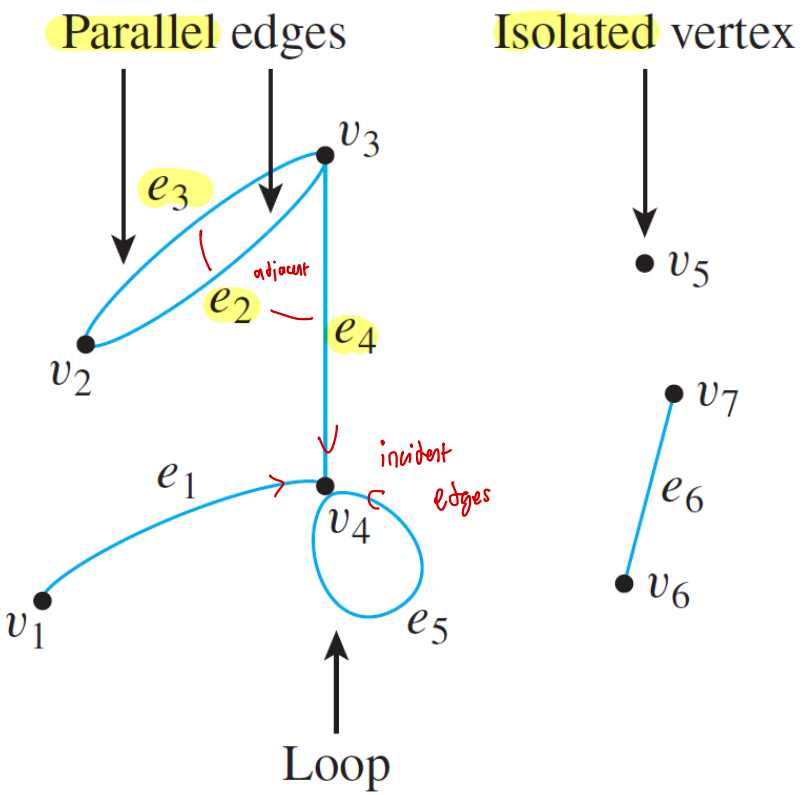
Pairwise

mutually.

# Summary



An **undirected graph** $G = (V, E)$ consists of
- a set of vertices $V = \{v_1, v_2, \cdots, v_n\}$, and
- a set of (undirected) edges $E = \{e_1, e_2, \cdots, e_k\}$.
- An (undirected) edge $e$ connecting $v_i$ and $v_j$ is denoted as $e = \{v_i, v_j\}$.




$V = \{v_1, v_2, v_3, v_4, v_5, v_6, v_7\}$
$E = \{e_1, e_2, e_3, e_4, e_5, e_6\}$

Connections:

$e_1 = \{v_1, v_4\}$
$e_2 = e_3 = \{v_2, v_3\}$
$e_4 = \{v_3, v_4\}$
$e_5 = \{v_4, v_4\}$
$e_6 = \{v_6, v_7\}$

Edges incident on $v_4$: $e_1$, $e_4$ and $e_5$.
Vertices adjacent to $v_4$: $v_1$, $v_3$ and $v_4$.
Edges adjacent to $e_2$: $e_3$ and $e_4$.

# Summary



## Definition: Undirected Graph

An undirected **graph** $G$ consists of 2 finite sets: a nonempty set $V$ of **vertices** and a set $E$ of **edges**, where each (undirected) edge is associated with a set consisting of either one or two vertices called its **endpoints**.

An edge is said to **connect** its endpoints; two vertices that are connected by an edge are called **adjacent vertices**; and a vertex that is an endpoint of a loop is said to be **adjacent to itself**.

An edge is said to be **incident on** each of its endpoints, and two edges incident on the same endpoint are called **adjacent edges**.

We write $e = \{v, w\}$ for an undirected edge $e$ incident on vertices $v$ and $w$.

## Definition: Directed Graph

A **directed graph**, or **digraph**, $G$, consists of 2 finite sets: a nonempty set $V$ of **vertices** and a set $E$ of **directed edges**, where each (directed) edge is associated with an ordered pair of vertices called its **endpoints**.

We write $e = (v, w)$ for a directed edge $e$ from vertex $v$ to vertex $w$.

ordered pairs

# Summary

## 10.1 Definitions and Basic Properties

### Definition: Simple Graph

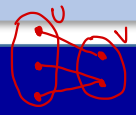
A **simple graph** is an undirected graph that does not have any loops or parallel edges. (That is, there is at most one edge between each pair of distinct vertices.)

### Definition: Complete Graph

A **complete graph** on ***n* vertices**, $n > 0$, denoted $K_n$, is a simple graph with $n$ vertices and exactly one edge connecting each pair of distinct vertices.

### Definition: Bipartite Graph

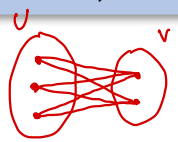
A **bipartite graph** (or bigraph) is a simple graph whose vertices can be divided into two disjoint sets $U$ and $V$ such that every edge connects a vertex in $U$ to one in $V$.




### Definition: Complete Bipartite Graph

A **complete bipartite graph** is a bipartite graph on two disjoint sets $U$ and $V$ such that every vertex in $U$ connects to every vertex in $V$.

If $|U| = m$ and $|V| = n$, the complete bipartite graph is denoted as $K_{m,n}$.



# Summary

## 10.1 Definitions and Basic Properties

### Definition: Subgraph of a Graph

A graph $H$ is said to be a **subgraph** of graph $G$ iff every vertex in $H$ is also a vertex in $G$, every edge in $H$ is also an edge in $G$, and every edge in $H$ has the same endpoints as it has in $G$.

### Definition: Degree of a Vertex and Total Degree of a Graph

Let $G$ be a graph and $v$ a vertex of $G$. The **degree** of $v$, denoted **deg($v$)**, equals the number of edges that are incident on $v$, with an edge that is a loop counted twice.

The **total degree of $G$** is the sum of the degrees of all the vertices of $G$.

### Theorem 10.1.1 The Handshake Theorem

If the vertices of $G$ are $v_1, v_2, \ldots, v_n$, where $n \geq 0$, then the total degree of $G$

$= \deg(v_1) + \deg(v_2) + \ldots + \deg(v_n) = 2 \times$ (the number of edges of $G$).

### Corollary 10.1.2

The total degree of a graph is even.

### Proposition 10.1.3

In any graph there are an even number of vertices of odd degree.

# Summary



## Definition: Indegree and outdegree of a Vertex of a Directed Graph

Let $G=(V,E)$ be a directed graph and $v$ a vertex of $G$. The **indegree** of $v$, denoted $\mathbf{deg^-(v)}$, is the number of directed edges that end at $v$. The **outdegree** of $v$, denoted $\mathbf{deg^+(v)}$, is the number of directed edges that originate from $v$.

Note that $$\sum_{v \in V} deg^-(v) = \sum_{v \in V} deg^+(v) = |E|$$

sum of all indegrees = sum of all outdegrees = number of all edges

# Summary



## Definitions

Let $G$ be a graph, and let $v$ and $w$ be vertices of $G$.

A **walk from $v$ to $w$** is a finite alternating sequence of adjacent vertices and edges of $G$. Thus a walk has the form $v_0\, e_1\, v_1\, e_2 \ldots v_{n-1}\, e_n\, v_n$, where the $v$'s represent vertices, the $e$'s represent edges, $v_0=v$, $v_n=w$, and for all $i \in \{1, 2, \ldots, n\}$, $v_{i-1}$ and $v_i$ are the endpoints of $e_i$. The number of edges, $n$, is the **length** of the walk.

The **trivial walk** from $v$ to $v$ consists of the single vertex $v$.

A **trail from $v$ to $w$** is a walk from $v$ to $w$ that does not contain a repeated edge. no repeat edge

A **path from $v$ to $w$** is a trail that does not contain a repeated vertex. no repeat edge & vertex

A **closed walk** is a walk that starts and ends at the same vertex.

**Circuit** (or **cycle**): Let $n \in \mathbb{Z}_{\geq 3}$. An undirected graph $G(V, E)$ where $V = \{x_1, x_2, \cdots, x_n\}$ and $E = \{\{x_1, x_2\}, \{x_2, x_3\}, \cdots, \{x_{n-1}, x_n\}, \{x_n, x_1\}\}$ is called **a circuit/cycle**. no repeat edge.

A **simple circuit** (or **simple cycle**) is a circuit that does not have any other repeated vertex except the first and last. no repeat vertex except first & last. & no repeat edge.

An undirected graph is **cyclic** if it contains a loop or a cycle; otherwise, it is **acyclic**.

# Summary



## Definition: Connectedness

**Two vertices** $v$ and $w$ of a graph $G$ are **connected** iff there is a walk from $v$ to $w$.

**The graph $G$ is connected** iff given *any* two vertices $v$ and $w$ in $G$, there is a walk from $v$ to $w$. Symbolically, $G$ is connected iff $\forall$ vertices $v, w \in V(G)$, $\exists$ a walk from $v$ to $w$.

## Lemma 10.2.1

Let $G$ be a graph.

a. If $G$ is connected, then any two distinct vertices of $G$ can be connected by a path.
b. If vertices $v$ and $w$ are part of a circuit in $G$ and one edge is removed from the circuit, then there still exists a trail from $v$ to $w$ in $G$.
c. If $G$ is connected and $G$ contains a circuit, then an edge of the circuit can be removed without disconnecting $G$.

## Definition: Connected Component

A graph $H$ is a **connected component** of a graph $G$ iff

1. The graph $H$ is a subgraph of $G$;
2. The graph $H$ is connected; and
3. No connected subgraph of $G$ has $H$ as a subgraph and contains vertices or edges that are not in $H$.

# Summary



## Definitions: Euler Circuit and Eulerian Graph

Let $G$ be a graph. An **Euler circuit** for $G$ is a circuit that contains every vertex and every edge of $G$. contains every vertex & edge. (vertex can be repeated, edge cannot).

An **Eulerian graph** is a graph that contains an Euler circuit.

## Theorem 10.2.2

If a graph has an Euler circuit, then every vertex of the graph has positive even degree.

## Contrapositive Version of Theorem 10.2.2

If some vertex of a graph has odd degree, then the graph doesn't have an Euler circuit.

## Theorem 10.2.3

If a graph $G$ is connected and the degree of every vertex of $G$ is a positive even integer, then $G$ has an Euler circuit.

## Theorem 10.2.4

A graph $G$ has an Euler circuit iff $G$ is connected and every vertex of $G$ has positive even degree.

# Summary



## Definition: Euler Trail

Let $G$ be a graph, and let $v$ and $w$ be two distinct vertices of $G$. An **Euler trail/path from $v$ to $w$** is a sequence of adjacent edges and vertices that starts at $v$, ends at $w$, passes through every vertex of $G$ at least once, and traverses every edge of $G$ exactly once.

Same as circuit, no need to end at same point. (2 end pts odd degree, rest even).

## Corollary 10.2.5

Let $G$ be a graph, and let $v$ and $w$ be two distinct vertices of $G$. There is an Euler trail from $v$ to $w$ iff $G$ is connected, $v$ and $w$ have odd degree, and all other vertices of $G$ have positive even degree.

Number of Hamiltonian paths: (undirected).

Complete graph: $n!$

Complete bipartite graph: $(n!)^2$

number of Hamiltonian cycles:

Complete graph: $\frac{1}{2}(n-1)!$

Complete bipartite graph: $\frac{1}{2}n!(n-1)!$

# Summary



## Definitions: Hamiltonian Circuit and Hamiltonian Graph

Given a graph *G*, a **Hamiltonian circuit** for *G* is a simple circuit that includes every vertex of *G*. (That is, every vertex appears exactly once, except for the first and the last, which are the same.) every vertex once & no repeat edge.

A **Hamiltonian graph** (also called **Hamilton graph**) is a graph that contains a Hamiltonian circuit.

## Proposition 10.2.6

If a graph *G* has a Hamiltonian circuit, then *G* has a subgraph *H* with the following properties:

1. *H* contains every vertex of *G*.
2. *H* is connected.
3. *H* has the same number of edges as vertices.
4. Every vertex of *H* has degree 2.

# Summary



## Definition: Adjacency Matrix of a Directed Graph

Let $G$ be a directed graph with ordered vertices $v_1, v_2, \ldots v_n$. The **adjacency matrix of $G$** is the $n \times n$ matrix $\mathbf{A} = (a_{ij})$ over the set of non-negative integers such that

$a_{ij}$ = the number of arrows from $v_i$ to $v_j$ for all $i, j = 1, 2, \ldots, n$.


## Definition: Adjacency Matrix of an Undirected Graph

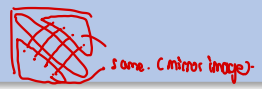
Let $G$ be an undirected graph with ordered vertices $v_1, v_2, \ldots v_n$. The **adjacency matrix of $G$** is the $n \times n$ matrix $\mathbf{A} = (a_{ij})$ over the set of non-negative integers such that

$a_{ij}$ = the number of edges connecting $v_i$ and $v_j$ for all $i, j = 1, 2, \ldots, n$.

## Definition: Symmetric Matrix

An $n \times n$ square matrix $A = (a_{ij})$ is called **symmetric** iff for all $i, j = 1, 2, \ldots, n$,

$$a_{ij} = a_{ji}.$$



# Summary



## Definition: $n^{th}$ Power of a Matrix

For any $n \times n$ matrix **A**, the **powers of A** are defined as follows:

$\mathbf{A}^0 = \mathbf{I}$ where **I** is the $n \times n$ identity matrix

$\mathbf{A}^n = \mathbf{A}\,\mathbf{A}^{n-1}$ for all integers $n \geq 1$

## Theorem 10.3.2

If $G$ is a graph with vertices $v_1, v_2, \ldots, v_m$ and **A** is the adjacency matrix of $G$, then for each positive integer $n$ and for all integers $i, j = 1, 2, \ldots, m$,

the $ij$-th entry of $\mathbf{A}^n$ = the number of walks of length $n$ from $v_i$ to $v_j$.

# Summary



## Definition: Isomorphic Graph

Let $G = (V_G, E_G)$ and $G' = (V_{G'}, E_{G'})$ be two graphs.

different arrangement but same everything else.

**$G$ is isomorphic to $G'$**, denoted $G \cong G'$, if and only if there exist bijections $g: V_G \to V_{G'}$ and $h: E_G \to E_{G'}$ that preserve the edge-endpoint functions of $G$ and $G'$ in the sense that for all $v \in V_G$ and $e \in E_G$,

$v$ is an endpoint of $e \Leftrightarrow g(v)$ is an endpoint of $h(e)$.

## Alternative definition

Let $G = (V_G, E_G)$ and $G' = (V_{G'}, E_{G'})$ be two graphs.

**$G$ is isomorphic to $G'$** if and only if there exists a permutation $\pi: V_G \to V_{G'}$ such that $\{u, v\} \in E_G \Leftrightarrow \{\pi(u), \pi(v)\} \in E_{G'}$.

## Theorem 10.4.1 Graph Isomorphism is an Equivalence Relation

Let $S$ be a set of graphs and let $\cong$ be the relation of graph isomorphism on $S$.
Then $\cong$ is an equivalence relation on $S$.

# Summary



## Definition: Planar Graph

A **planar graph** is a graph that can be drawn on a (two-dimensional) plane without edges crossing.

## Euler's Formula

For a connected planar simple graph $G = (V, E)$ with $e = |E|$ and $v = |V|$, if we let $f$ be the number of faces, then

$$f = e - v + 2$$

✳ Notes: A $K_n$ graph has $\binom{n}{2} = \frac{n(n-1)}{2}$ edges

# Summary



## Definition: Tree

A **graph** is said to be **circuit-free** iff it has no circuits.

A graph is called a **tree** if it is circuit-free and connected.

A **trivial tree** is a graph that consists of a single vertex.

A graph is called a **forest** iff it is circuit-free and not connected.

## Definitions: Terminal vertex (leaf) and internal vertex

Let $T$ be a tree. If $T$ has only one or two vertices, then each is called a **terminal vertex** (or **leaf**). If $T$ has at least three vertices, then a vertex of degree 1 in $T$ is called a **terminal vertex** (or **leaf**), and a vertex of degree greater than 1 in $T$ is called an **internal vertex**.

# Summary

## 10.5 Trees

### Lemma 10.5.1

Any non-trivial tree has at least one vertex of degree 1.

### Theorem 10.5.2

Any tree with $n$ vertices ($n > 0$) has $n - 1$ edges.

### Lemma 10.5.3

If $G$ is any connected graph, $C$ is any circuit in $G$, and one of the edges of $C$ is removed from $G$, then the graph that remains is still connected.

### Theorem 10.5.4

If $G$ is a connected graph with $n$ vertices and $n - 1$ edges, then $G$ is a tree.

# Summary



## Definitions: Rooted Tree, Level, Height

A **rooted tree** is a tree in which there is one vertex that is distinguished from the others and is called the **root**.

The **level** of a vertex is the number of edges along the unique path between it and the root. start from 0.

The **height** of a rooted tree is the maximum level of any vertex of the tree.

## Definitions: Child, Parent, Sibling, Ancestor, Descendant

Given the root or any internal vertex $v$ of a rooted tree, the **children** of $v$ are all those vertices that are adjacent to $v$ and are one level farther away from the root than $v$.

If $w$ is a child of $v$, then $v$ is called the **parent** of $w$, and two distinct vertices that are both children of the same parent are called **siblings**.

Given two distinct vertices $v$ and $w$, if $v$ lies on the unique path between $w$ and the root, then $v$ is an **ancestor** of $w$, and $w$ is a **descendant** of $v$.

# Summary



## Definitions: Binary Tree, Full Binary Tree

A **binary tree** is a rooted tree in which every parent has at most two children. Each child is designated either a **left child** or a **right child** (but not both), and every parent has at most one left child and one right child.

A **full binary tree** is a binary tree in which each parent has exactly two children.

## Definitions: Left Subtree, Right Subtree

Given any parent $v$ in a binary tree $T$, if $v$ has a left child, then the **left subtree** of $v$ is the binary tree whose root is the left child of $v$, whose vertices consist of the left child of $v$ and all its descendants, and whose edges consist of all those edges of $T$ that connect the vertices of the left subtree.

The **right subtree** of $v$ is defined analogously.

# Summary



## Theorem 10.6.1: Full Binary Tree Theorem

If $T$ is a full binary tree with $k$ internal vertices, then $T$ has a total of $2k + 1$ vertices and has $k + 1$ terminal vertices (leaves).

relation between number of vertices of a full binary tree.

## Theorem 10.6.2

For non-negative integers $h$, if $T$ is any binary tree with height $h$ and $t$ terminal vertices (leaves), then

leaves — height

$$t \leq 2^h$$

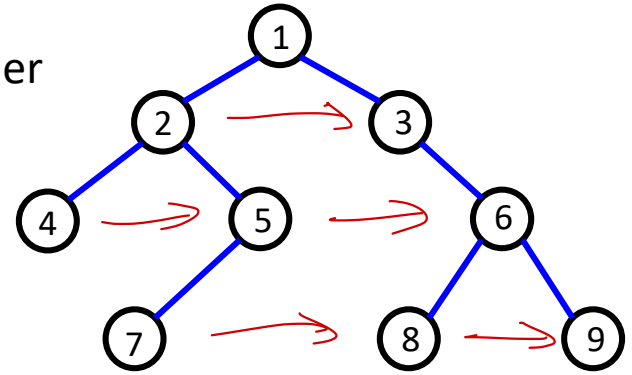
Equivalently,

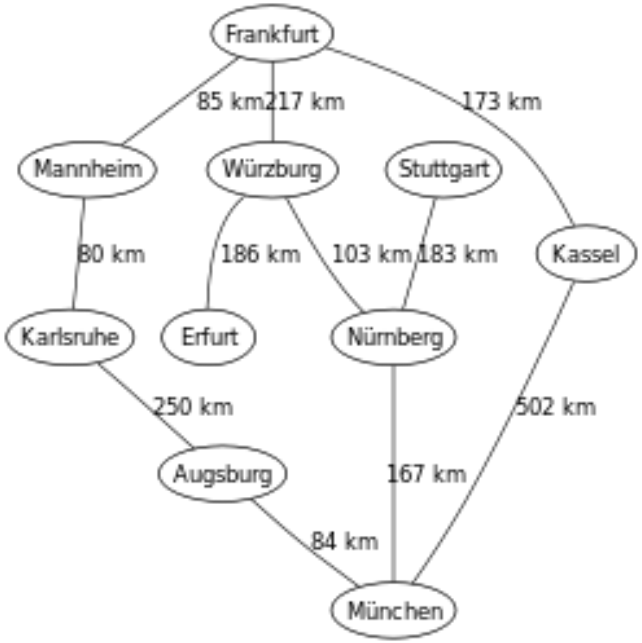
$$\log_2 t \leq h$$

# Breadth-First Search

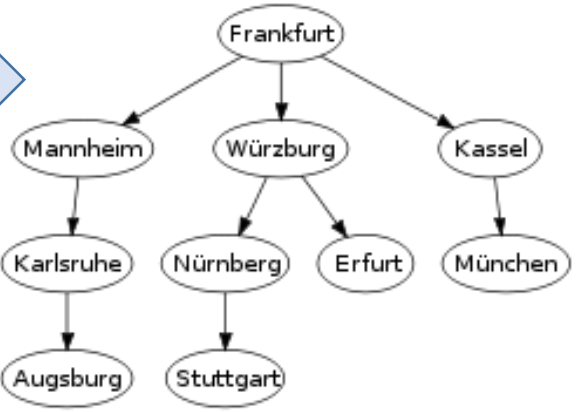
In breadth-first search (by E.F. Moore), it starts at the root and visits its adjacent vertices, and then moves to the next level.

The figure shows the order of the vertices visited.




BFS





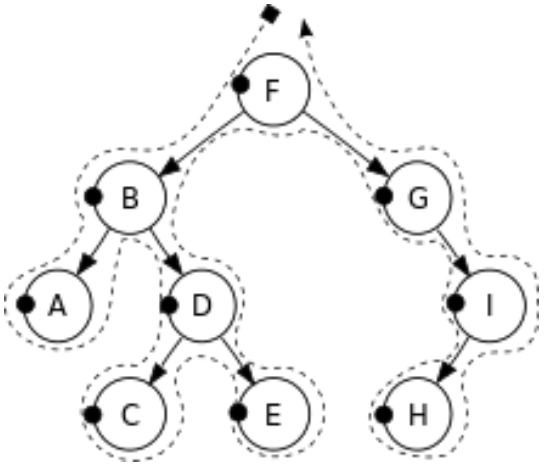

Acknowledgement: Wikipedia https://en.wikipedia.org/wiki/Breadth-first_search

# Depth-First Search

There are three types of depth-first traversal:

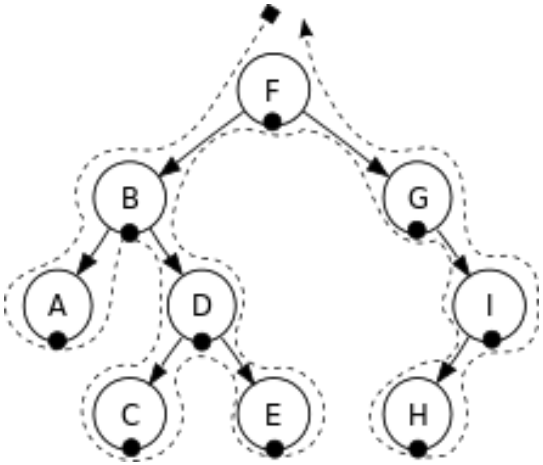
- Pre-order
  - Print the data of the root (or current vertex)
  - Traverse the left subtree by recursively calling the pre-order function
  - Traverse the right subtree by recursively calling the pre-order function
- In-order
  - Traverse the left subtree by recursively calling the in-order function
  - Print the data of the root (or current vertex)
  - Traverse the right subtree by recursively calling the in-order function
- Post-order
  - Traverse the left subtree by recursively calling the post-order function
  - Traverse the right subtree by recursively calling the post-order function
  - Print the data of the root (or current vertex)

# Depth-First Search



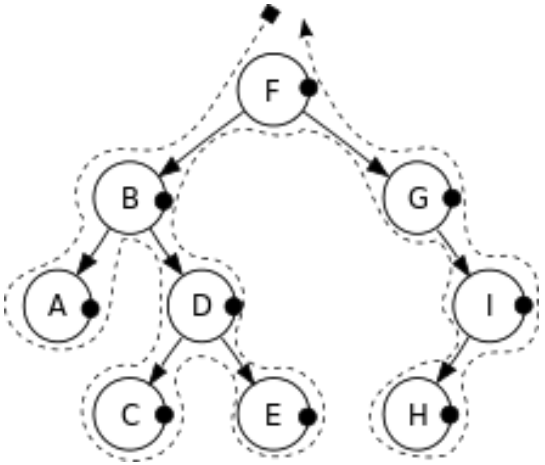

Pre-order:

F, B, A, D, C, E, G, I, H




In-order:

A, B, C, D, E, F, G, H, I




Post-order:

A, C, E, D, B, H, I, G, F

Acknowledgement: Wikipedia https://en.wikipedia.org/wiki/Tree_traversal

# Summary



## Definition: Spanning Tree

A **spanning tree** for a graph $G$ is a subgraph of $G$ that contains every vertex of $G$ and is a tree.

## Proposition 10.7.1

1. Every connected graph has a spanning tree.
2. Any two spanning trees for a graph have the same number of edges.

## Definitions: Weighted Graph, Minimum Spanning Tree

A **weighted graph** is a graph for which each edge has an associated positive real number **weight**. The sum of the weights of all the edges is the **total weight** of the graph.

A **minimum spanning tree** for a connected weighted graph is a spanning tree that has the least possible total weight compared to all other spanning trees for the graph.

If $G$ is a weighted graph and $e$ is an edge of $G$, then $\boldsymbol{w(e)}$ denotes the weight of $e$ and $\boldsymbol{w(G)}$ denotes the total weight of $G$.

## Algorithm 10.7.1 Kruskal

add in the edge.

Input: $G$ [a connected weighted graph with $n$ vertices]

Algorithm:

1. Initialize $T$ to have all the vertices of $G$ and no edges.
2. Let $E$ be the set of all edges of $G$, and let $m = 0$.
3. While ($m < n - 1$)
   - 3a. Find an edge $e$ in $E$ of least weight.
   - 3b. Delete $e$ from $E$.
   - 3c. If addition of $e$ to the edge set of $T$ does not produce a circuit, then add $e$ to the edge set of $T$ and set $m = m + 1$

   End while

Output: $T$ [$T$ is a minimum spanning tree for $G$]

## Algorithm 10.7.2 Prim

Input: $G$ [a connected weighted graph with $n$ vertices]

Algorithm:

1. Pick a vertex $v$ of $G$ and let $T$ be the graph with this vertex only.
2. Let $V$ be the set of all vertices of $G$ except $v$.
3. For $i = 1$ to $n - 1$
   - 3a. Find an edge $e$ of $G$ such that (1) $e$ connects $T$ to one of the vertices in $V$, and (2) $e$ has the least weight of all edges connecting $T$ to a vertex in $V$. Let $w$ be the endpoint of $e$ that is in $V$.
   - 3b. Add $e$ and $w$ to the edge and vertex sets of $T$, and delete $w$ from $V$.

Output: $T$ [$T$ is a minimum spanning tree for $G$]