General Tips

When asked to prove or disprove, always try to disprove first.

When there is a conditional statement, try to get *true* → *false* to disprove

Chapter 1 / 4

- $\mathbb{N}$ $(\mathbb{Z}_{\geq 0})$: the set of all natural numbers
  $\{$ 0, 1, 2, 3, …$\}$
  $\mathbb{Z}$: the set of all integers
  $\mathbb{Q}$: the set of all rational numbers
  $\mathbb{R}$: the set of all real numbers
  $\mathbb{C}$: the set of all complex numbers (note: we will not cover this)
  $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

  Irrationality means $\sim\mathbb{Q}$ but in $\mathbb{R}$.
  → Proof by contradiction
- $\mathbb{Z}^{+}$: the set of all positive integers
  $\mathbb{R}^{-}$: the set of all negative real numbers
  $\mathbb{Z}_{\geq 12}$: the set of all integers greater than or equal to 12
- Note that 0 is neither **negative** nor **positive**

Proofs

- Direct proof
- Proof by construction
- Disproof by counterexample
- Proof by exhaustion
- Proof by contradiction
- Proof by contraposition
- Proof by mathematical induction
- Combinatorial proof

Some properties of integers/real numbers

- Closure: Integers are closed under addition and multiplication, i.e. $x + y \in \mathbb{Z}$ and $xy \in \mathbb{Z}$.
- Commutativity: Addition and multiplication are commutative, i.e. $x + y = y + x$ and $xy = yx$.
- Associativity: Addition and multiplication are associative, i.e. $x + y + z = (x + y) + z = x + (y + z)$ and $xyz = (xy)z = x(yz)$.
- Distributivity: Multiplication is distributive over addition (but not the other way round), i.e. $x(y + z) = xy + xz$ and $(y + z)x = yx + zx$.
- Trichotomy: Exactly one of the following is true:
  $x = y$, or $x < y$, or $x > y$.

Assumption 1: For CS1231S, you may assume that every integer is even or odd, but not both.

Assumption 2: Every rational can be reduced to a fraction in its lowest term.

Divisibility:

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

Theorem 4.7.1 (5th: 4.8.1)

Irrationality of $\sqrt{2}$

Proposition 4.6.4 (5th: 4.7.4)

For all integers n, if n^2 is even then n is even.

Definition of Even and Odd

n is even $\Leftrightarrow \exists$ an integer k such that $n = 2k$.

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

0 is even

Definition of 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: $(n > 1) \land \forall r, s \in \mathbb{Z}^{+}$,

$\big(n = rs \rightarrow (r = 1 \land s = n) \lor (r = n \land s = 1)\big)$.

n is composite: $\exists r, s \in \mathbb{Z}^{+}\ \big(n = rs \land (1 < r < n) \land (1 < s < n)\big)$.

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 $b \neq 0$.

Theorem 4.2.1 (5th: 4.3.1)

Every integer is a rational number.

Theorem 4.2.2 (5th: 4.3.2)

The sum of any two rational numbers is rational.

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 $a \leq b$.

Theorem 4.3.2 (5th: 4.4.2) Divisors of 1

The only divisors of 1 are 1 and -1.

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 $a \mid c$.

Theorem 4.6.1 (5th: 4.7.1)

There is no greatest integer.

Theorem 4.4.1 The Quotient-Remainder Theorem

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

$n = dq + r$ and $0 \leq r < d$.

By the quotient-remainder theorem, every integer *n* can be written in exactly one of the three forms: *n* = 3*k*, or *n* = 3*k*+1, or *n* = 3*k* + 2 for some integer *k*.

Chapter 2

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 ~*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 2.1.6 (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 $\boldsymbol{P \equiv Q}$.

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 ~*q* then ~*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 ~*p* then ~*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 "$\sim q \to \sim p$"

Or, equivalently,

"if *p* then *q*" or "$p \to q$"

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

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*" or "$r \to s$"

"*r* is a necessary condition for *s*" means "if not *r* then not *s*"

or "if *s* then *r*" or "$s \to r$"

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**.

Order of Operations

~ / ∧∨ / →↔

Only If/ If / Necessary / Sufficient

p only if q	p → q / ~q → ~p
p if q	q → p
p is necessary for q	q → p / ~p → ~q
p is sufficient for q	p → q

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

Normal:	p → q
Contrapositive:	~q → ~p (same as p → q)
Converse:	q → p
Inverse:	~p → ~q

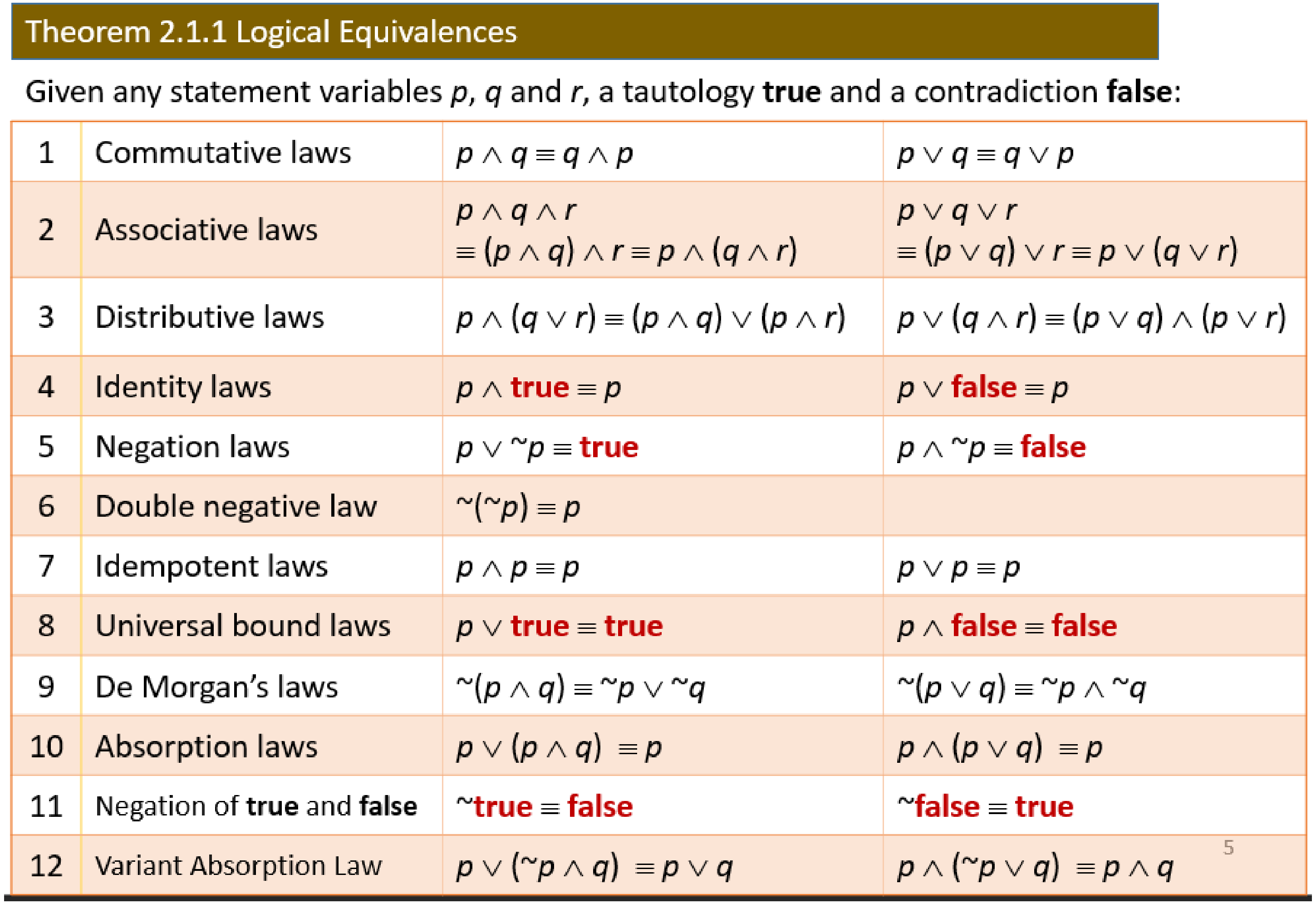
Converse Error
Inverse Error

Notes:

When given p and q and an implication, or rules of inference, always try to find a counterexample using the conclusion (therefore p→q) where p is false and q is true

False ≡ contradiction
True ≡ Tautology
q !≡ false
q !≡ true

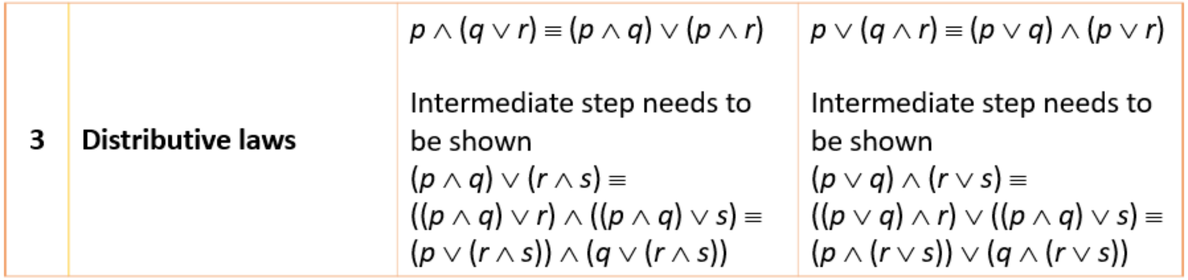
To prove not tautology or contradiction, not sufficient to prove that the result is equivalent to p. Need to show that p can possibly be False/True which is a counterexample to always true.



Theorem 2.1.1 Logical Equivalences

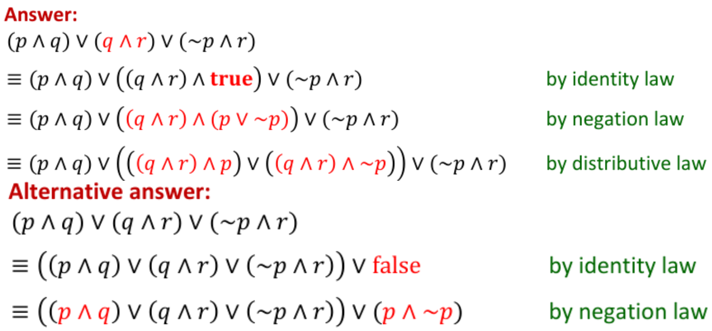
Given any statement variables *p*, *q* and *r*, a tautology **true** and a contradiction **false**:

1	Commutative laws	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
2	Associative laws	$p \wedge q \wedge r$ $\equiv (p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$p \vee q \vee r$ $\equiv (p \vee q) \vee r \equiv p \vee (q \vee r)$
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	$p \wedge \textbf{true} \equiv p$	$p \vee \textbf{false} \equiv p$
5	Negation laws	$p \vee {\sim}p \equiv \textbf{true}$	$p \wedge {\sim}p \equiv \textbf{false}$
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	$p \vee \textbf{true} \equiv \textbf{true}$	$p \wedge \textbf{false} \equiv \textbf{false}$
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**	${\sim}\textbf{true} \equiv \textbf{false}$	${\sim}\textbf{false} \equiv \textbf{true}$
12	Variant Absorption Law	$p \vee ({\sim}p \wedge q) \equiv p \vee q$	$p \wedge ({\sim}p \vee q) \equiv p \wedge q$



3	**Distributive laws**	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ Intermediate step needs to be shown $(p \wedge q) \vee (r \wedge s) \equiv$ $((p \wedge q) \vee r) \wedge ((p \wedge q) \vee s) \equiv$ $(p \vee (r \wedge s)) \wedge (q \vee (r \wedge s))$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ Intermediate step needs to be shown $(p \vee q) \wedge (r \vee s) \equiv$ $((p \vee q) \wedge r) \vee ((p \wedge q) \vee s) \equiv$ $(p \wedge (r \vee s)) \vee (q \wedge (r \vee s))$

Using Identity law (AY21/22S1 Midterm)



Answer:

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

$\equiv (p \wedge q) \vee \big((q \wedge r) \wedge \mathbf{true}\big) \vee (\sim p \wedge r)$ by identity law

$\equiv (p \wedge q) \vee \big((q \wedge r) \wedge (p \vee \sim p)\big) \vee (\sim p \wedge r)$ by negation law

$\equiv (p \wedge q) \vee \Big(\big((q \wedge r) \wedge p\big) \vee \big((q \wedge r) \wedge \sim p\big)\Big) \vee (\sim p \wedge r)$ by distributive law

Alternative answer:

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

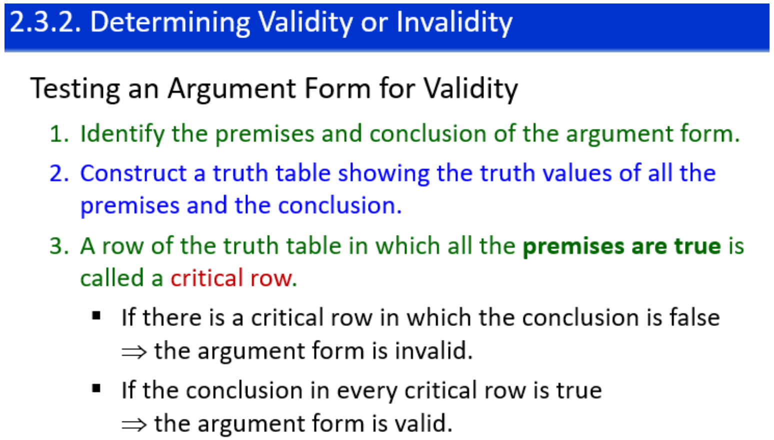
$\equiv \big((p \wedge q) \vee (q \wedge r) \vee (\sim p \wedge r)\big) \vee \text{false}$ by identity law

$\equiv \big((p \wedge q) \vee (q \wedge r) \vee (\sim p \wedge r)\big) \vee (p \wedge \sim p)$ by negation law

Premise A ∧ Premise B → Conclusion

Premise A ∧ Premise B != Conclusion

p → q ≡ ~p ∨ q (Implication Law)
~(p → q) ≡ p ∧ ~q (L2 E2.2.3)

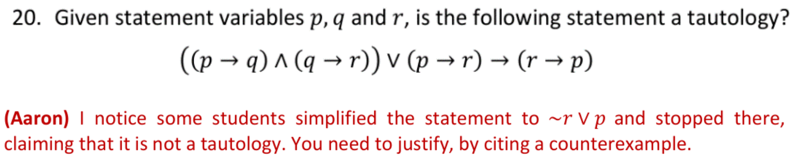


2.3.2. Determining Validity or Invalidity

Testing an Argument Form for Validity

1. Identify the premises and conclusion of the argument form.
2. Construct a truth table showing the truth values of all the premises and the conclusion.
3. A row of the truth table in which all the **premises are true** is called a critical row.
   - If there is a critical row in which the conclusion is false ⇒ the argument form is invalid.
   - If the conclusion in every critical row is true ⇒ the argument form is valid.

20S1 midterm: when proving something is not a tautology, don't just simplify it and stop there. Give **a counterexample**



20. Given statement variables p, q and r, is the following statement a tautology?

$$\big((p \to q) \wedge (q \to r)\big) \vee (p \to r) \to (r \to p)$$

(Aaron) I notice some students simplified the statement to $\sim r \vee p$ and stopped there, claiming that it is not a tautology. You need to justify, by citing a counterexample.

r ^ ~p != true.
But r ^ ~p does not prove not tautology

Same for proving something is not a contradiction. Give a counterexample to show it is not false

A tautology means "always true". Not "true" itself

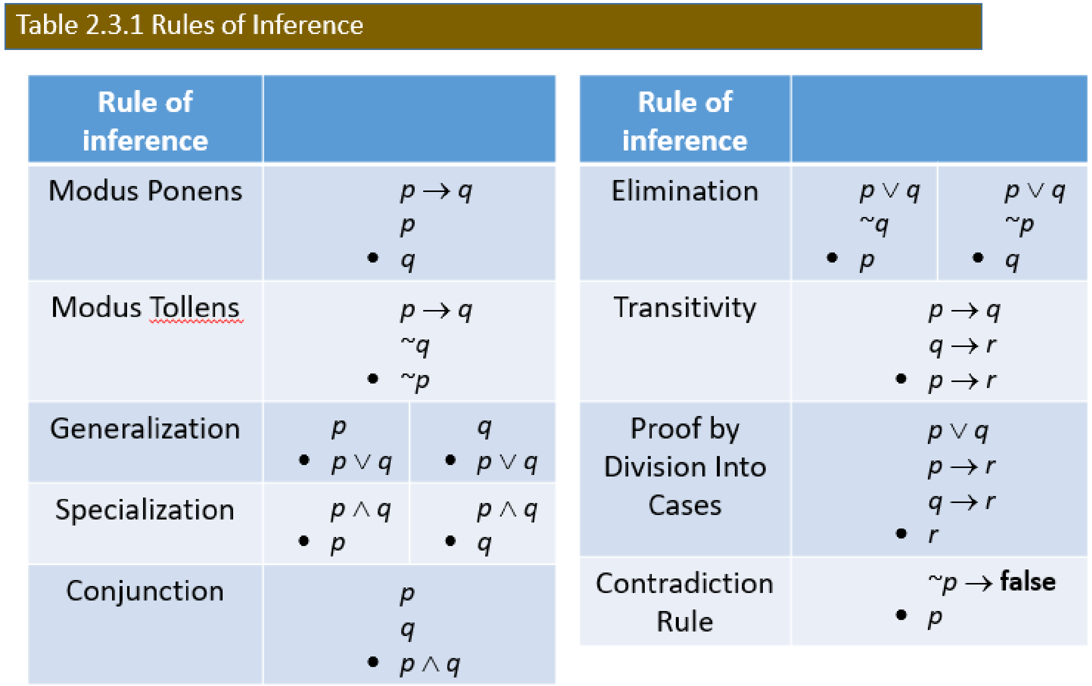
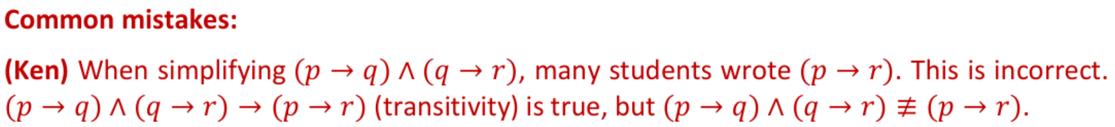


Table 2.3.1 Rules of Inference

Rule of inference		
Modus Ponens	$p \to q$ p • q	
Modus Tollens	$p \to q$ $\sim q$ • $\sim p$	
Generalization	p • $p \vee q$	q • $p \vee q$
Specialization	$p \wedge q$ • p	$p \wedge q$ • q
Conjunction	p q • $p \wedge q$	

Rule of inference		
Elimination	$p \vee q$ $\sim q$ • p	$p \vee q$ $\sim p$ • q
Transitivity	$p \to q$ $q \to r$ • $p \to r$	
Proof by Division Into Cases	$p \vee q$ $p \to r$ $q \to r$ • r	
Contradiction Rule	$\sim p \to$ **false** • p	



Common mistakes:

(Ken) When simplifying $(p \to q) \wedge (q \to r)$, many students wrote $(p \to r)$. This is incorrect. $(p \to q) \wedge (q \to r) \to (p \to r)$ (transitivity) is true, but $(p \to q) \wedge (q \to r) \not\equiv (p \to r)$.

Chapter 3

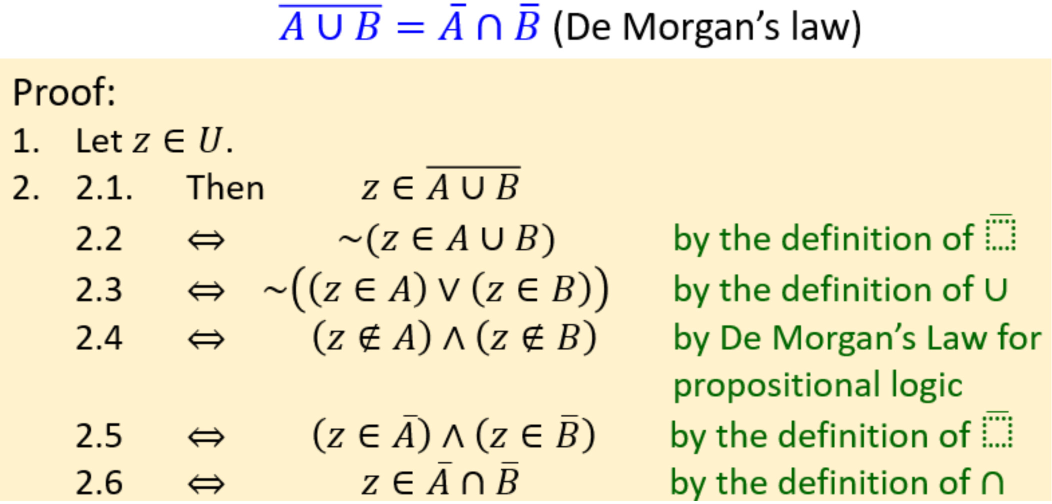
∀ for all
∃ there exists
∃! There exists unique

Negation of ∃ and ∀

~(∀x∈D, $P(x)$) ≡ ∃x∈D such that ~$P(x)$
~(∃x∈D such that $P(x)$) ≡ ∀x∈D, ~$P(x)$

~(∀x (P(x) ⟶ ∃y (Q(y)))
≡ ∃x ~(P(x) ⟶ ∃y (Q(y)))
≡ ∃x (~P(x) ∧ ~(∃y (Q(y))))
≡ ∃x (~P(x) ∧ ∀y (~Q(y)))

∀x∈D ($P(x)$ → $Q(x)$).
Its **contrapositive** is: ∀x∈D (~$Q(x)$ → ~$P(x)$).
Its **converse** is: ∀x∈D ($Q(x)$ → $P(x)$).
Its **inverse** is: ∀x∈D (~$P(x)$ → ~$Q(x)$).



$\overline{A \cup B} = \bar{A} \cap \bar{B}$ (De Morgan's law)

Proof:

1. Let $z \in U$.
2. 2.1. Then $z \in \overline{A \cup B}$
   2.2 ⇔ $\sim(z \in A \cup B)$ by the definition of ⬚
   2.3 ⇔ $\sim\big((z \in A) \lor (z \in B)\big)$ by the definition of ∪
   2.4 ⇔ $(z \notin A) \land (z \notin B)$ by De Morgan's Law for propositional logic
   2.5 ⇔ $(z \in \bar{A}) \land (z \in \bar{B})$ by the definition of ⬚
   2.6 ⇔ $z \in \bar{A} \cap \bar{B}$ by the definition of ∩

Chapter 5

Set-Roster Notation: {1,2,3}
Set builder notation: $\{x \in U : P(x)\}$
Replacement Notation: $\{t(x) : x \in A\}$

Subset
$A \subseteq B$ iff $\forall x\ (x \in A \Rightarrow x \in B)$

Proper Subset / Strict inclusion
$A \subsetneq B$, iff $A \subseteq B$ and $A \neq B$

Theorem 6.2.4

An empty set is a subset of every set, i.e. $\emptyset \subseteq A$ for all sets A.

Definition: Ordered Pair

An **ordered pair** is an expression of the form (x, y).
Two ordered pairs (a, b) and (c, d) are equal iff $a = c$ and $b = d$.
Symbolically: $(a, b) = (c, d) \Leftrightarrow (a = c) \wedge (b = d)$.

Cartesian Product

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

Definition: Set equality

Given sets A and B, A equals B, written $\boldsymbol{A} = \boldsymbol{B}$ iff every element of A is in B and every element of B is in A.

$A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$ or
$A = B \Leftrightarrow \forall x\ (x \in A \Leftrightarrow x \in B)$

1. Let sets X and Y be given. To prove $X = Y$:
2. ($\subseteq$) Prove that $X \subseteq Y$.
3. ($\supseteq$) Prove that $Y \subseteq X$ (or $X \supseteq Y$).
4. From (2) and (3), conclude that $X = Y$.

Definitions

1. The **union** of A and B, denoted $\boldsymbol{A} \cup \boldsymbol{B}$, is the set of all elements that are in at least one of A or B.
2. The **intersection** of A and B, denoted $\boldsymbol{A} \cap \boldsymbol{B}$, is the set of all elements that are common to both A and B.
3. The **difference** of B minus A (or **relative complement** of A in B), denoted $\boldsymbol{B} - \boldsymbol{A}$, or $\boldsymbol{B} \setminus \boldsymbol{A}$, is the set of all elements that are in B and not A.
4. The complement of A, denoted $\bar{\boldsymbol{A}}$, is the set of all elements in U that are not in A. (Note: Epp uses the notation A^c.)

Symbolically:

$$A \cup B = \{x \in U : x \in A \vee x \in B\},$$

$$A \cap B = \{x \in U : x \in A \wedge x \in B\},$$

$$B \setminus A = \{x \in U : x \in B \wedge x \notin A\},$$

$$\bar{A} = \{x \in U \mid x \notin A\}.$$

Intervals of Real Numbers

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

$$(a, b) = \{x \in \mathbb{R} : a < x < b\},\quad [a, b] = \{x \in \mathbb{R} : a \leq x \leq b\},$$

$$(a, b] = \{x \in \mathbb{R} : a < x \leq b\},\quad [a, b) = \{x \in \mathbb{R} : a \leq x < b\}.$$

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

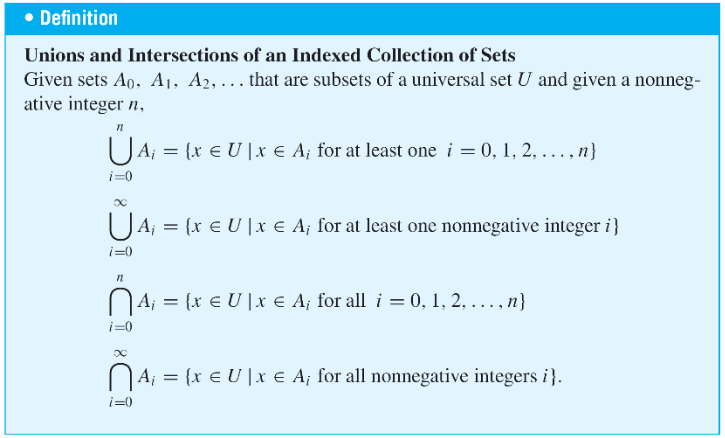
$$(a, \infty) = \{x \in \mathbb{R} : x > a\},\quad [a, \infty) = \{x \in \mathbb{R} : x \geq a\},$$

$$(-\infty, b) = \{x \in \mathbb{R} : x < b\},\quad (-\infty, b] = \{x \in \mathbb{R} : x \leq b\}.$$

Union/Intersection for More than 1 Set

$$\bigcup_{i=0}^{n} A_i = A_0 \cup A_1 \cup \cdots \cup A_n$$

$$\bigcap_{i=0}^{n} A_i = A_0 \cap A_1 \cap \cdots \cap A_n$$



• Definition

Unions and Intersections of an Indexed Collection of Sets

Given sets $A_0, A_1, A_2, \ldots$ that are subsets of a universal set U and given a nonnegative integer n,

$$\bigcup_{i=0}^{n} A_i = \{x \in U \mid x \in A_i \text{ for at least one } i = 0, 1, 2, \ldots, n\}$$

$$\bigcup_{i=0}^{\infty} A_i = \{x \in U \mid x \in A_i \text{ for at least one nonnegative integer } i\}$$

$$\bigcap_{i=0}^{n} A_i = \{x \in U \mid x \in A_i \text{ for all } i = 0, 1, 2, \ldots, n\}$$

$$\bigcap_{i=0}^{\infty} A_i = \{x \in U \mid x \in A_i \text{ for all nonnegative integers } i\}.$$

Disjoint

Two sets are **disjoint** iff they have no elements in common.

Symbolically: A and B are disjoint iff $A \cap B = \emptyset$.

Mutually Disjoint

Sets $A_1, A_2, A_3, \cdots$ are **mutually disjoint** (or **pairwise disjoint** or **nonoverlapping**) iff no two sets A_i and A_j with distinct subscripts have any elements in common, i.e. for all $i, j = 1,2,3, \cdots$

$$A_i \cap A_j = \emptyset \text{ whenever } i \neq j.$$

Power set

Given a set A, the **power set** of A, denoted $\mathcal{P}(A)$, is the set of all subsets of A.
A = {x, y}, $\mathcal{P}(A) = \{\emptyset, \{x\}, \{y\}, \{x, y\}\}$
A = $\emptyset$, $\mathcal{P}(A) = \{\emptyset\}$
A = $\{\emptyset\}$, $\mathcal{P}(A) = \{\emptyset, \{\emptyset\}\}$

Theorem 6.3.1

$|\mathcal{P}(A)| = 2^{|A|}$.

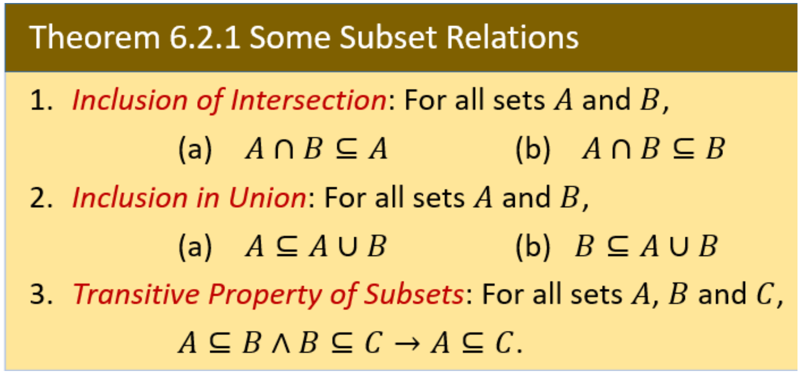
n-tuples

Equality of n-tuples:
$(x_1, x_2, \cdots, x_n) = (y_1, y_2, \cdots, y_n) \Leftrightarrow$
$x_1 = y_1, x_2 = y_2, \cdots, x_n = y_n$.

Cartesian Product

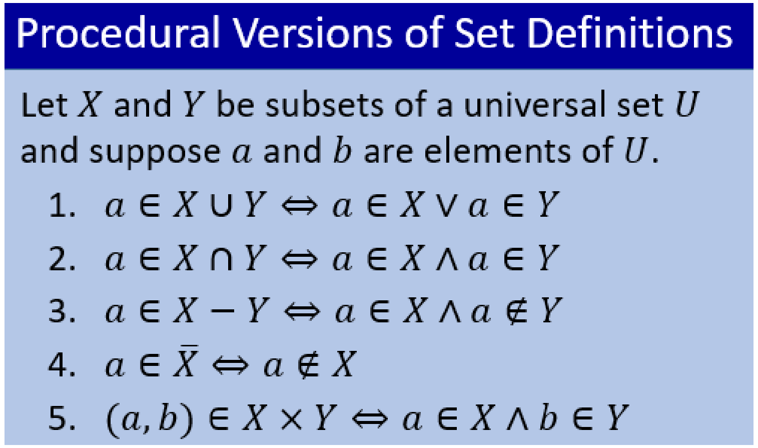
If A is a set, then $A^n = A \times A \times \cdots \times A$.
$\mathbb{Z}^3 = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} = \{(a, b, c) : a, b, c \in \mathbb{Z}\}$

$(A_1 \times A_2) \times A_3 = \{(u, v) : u \in A_1 \times A_2$ and $v \in A_3\}$



Theorem 6.2.1 Some Subset Relations

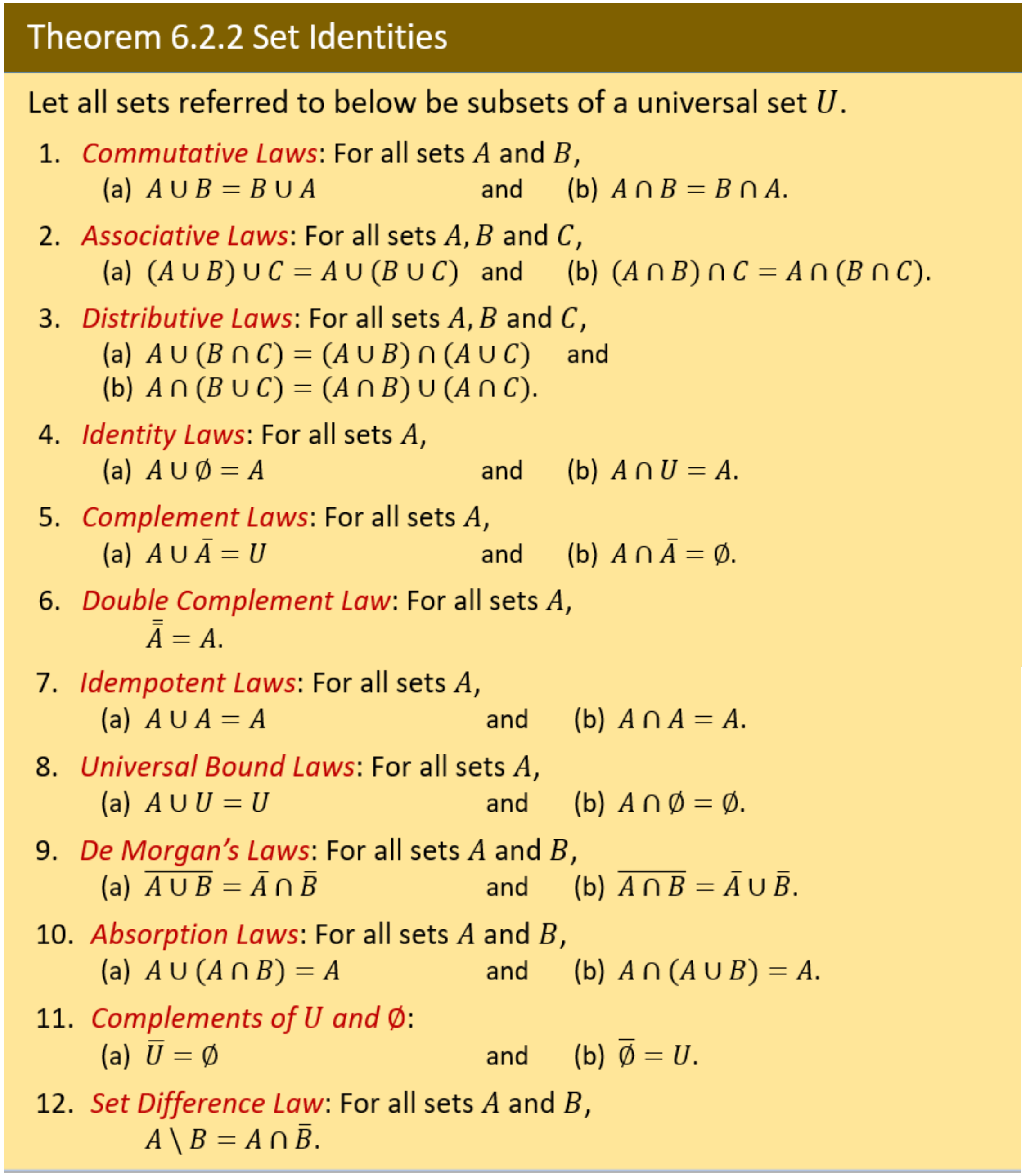
1. *Inclusion of Intersection*: For all sets A and B,
   (a) $A \cap B \subseteq A$ (b) $A \cap B \subseteq B$
2. *Inclusion in Union*: For all sets A and B,
   (a) $A \subseteq A \cup B$ (b) $B \subseteq A \cup B$
3. *Transitive Property of Subsets*: For all sets A, B and C,
   $A \subseteq B \wedge B \subseteq C \rightarrow A \subseteq C$.



Procedural Versions of Set Definitions

Let X and Y be subsets of a universal set U and suppose a and b are elements of U.

1. $a \in X \cup Y \Leftrightarrow a \in X \vee a \in Y$
2. $a \in X \cap Y \Leftrightarrow a \in X \wedge a \in Y$
3. $a \in X - Y \Leftrightarrow a \in X \wedge a \notin Y$
4. $a \in \bar{X} \Leftrightarrow a \notin X$
5. $(a, b) \in X \times Y \Leftrightarrow a \in X \wedge b \in Y$



Theorem 6.2.2 Set Identities

Let all sets referred to below be subsets of a universal set U.

1. *Commutative Laws*: For all sets A and B,
   (a) $A \cup B = B \cup A$ and (b) $A \cap B = B \cap A$.
2. *Associative Laws*: For all sets A, B and C,
   (a) $(A \cup B) \cup C = A \cup (B \cup C)$ and (b) $(A \cap B) \cap C = A \cap (B \cap C)$.
3. *Distributive Laws*: For all sets A, B and C,
   (a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ and
   (b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
4. *Identity Laws*: For all sets A,
   (a) $A \cup \emptyset = A$ and (b) $A \cap U = A$.
5. *Complement Laws*: For all sets A,
   (a) $A \cup \bar{A} = U$ and (b) $A \cap \bar{A} = \emptyset$.
6. *Double Complement Law*: For all sets A,
   $\bar{\bar{A}} = A$.
7. *Idempotent Laws*: For all sets A,
   (a) $A \cup A = A$ and (b) $A \cap A = A$.
8. *Universal Bound Laws*: For all sets A,
   (a) $A \cup U = U$ and (b) $A \cap \emptyset = \emptyset$.
9. *De Morgan's Laws*: For all sets A and B,
   (a) $\overline{A \cup B} = \bar{A} \cap \bar{B}$ and (b) $\overline{A \cap B} = \bar{A} \cup \bar{B}$.
10. *Absorption Laws*: For all sets A and B,
    (a) $A \cup (A \cap B) = A$ and (b) $A \cap (A \cup B) = A$.
11. *Complements of U and $\emptyset$*:
    (a) $\bar{U} = \emptyset$ and (b) $\bar{\emptyset} = U$.
12. *Set Difference Law*: For all sets A and B,
    $A \setminus B = A \cap \bar{B}$.

Appendix A

F1. *Commutative Laws* For all real numbers a and b,

$$a+b=b+a \quad \text{and} \quad ab=ba.$$

F2. *Associative Laws* For all real numbers a, b, and c,

$$(a+b)+c=a+(b+c) \quad \text{and} \quad (ab)c=a(bc).$$

F3. *Distributive Laws* For all real numbers a, b, and c,

$$a(b+c)=ab+ac \quad \text{and} \quad (b+c)a=ba+ca.$$

F4. *Existence of Identity Elements* There exist two distinct real numbers, denoted 0 and 1, such that for every real number a,

$$0+a=a+0=a \quad \text{and} \quad 1\cdot a=a\cdot 1=a.$$

F5. *Existence of Additive Inverses* For every real number a, there is a real number, denoted $-a$ and called the **additive inverse** of a, such that

$$a+(-a)=(-a)+a=0.$$

F6. *Existence of Reciprocals* For every real number $a \neq 0$, there is a real number, denoted $1/a$ or a^{-1}, called the **reciprocal** of a, such that

$$a\cdot\left(\frac{1}{a}\right)=\left(\frac{1}{a}\right)\cdot a=1.$$

Ord1. For any real numbers a and b, if a and b are positive, so are $a+b$ and ab.

Ord2. For every real number $a \neq 0$, either a is positive or $-a$ is positive but not both.

Ord3. The number 0 is not positive.

Definition

Given real numbers a and b,

$a<b$ means $b+(-a)$ is positive.
$a \leq b$ means $a<b$ or $a=b$.
If $a<0$, we say that a is **negative**.

$b>a$ means $a<b$.
$b \geq a$ means $a \leq b$.
If $a \geq 0$, we say that a is **nonnegative**.

T3. $b-a=b+(-a)$.

T4. $-(-a)=a$.

T5. $a(b-c)=ab-ac$.

T6. $0\cdot a=a\cdot 0=0$.

T7. *Cancellation Law for Multiplication* If $ab=ac$ and $a \neq 0$, then $b=c$. (In particular, this shows that the number 1 of Axiom F4 is unique.)

T8. *Possibility of Division* Given a and b with $a \neq 0$, there is exactly one x such that $ax=b$. This x is denoted by b/a and is called the **quotient** of b and a. In particular, $1/a$ is the reciprocal of a.

T9. If $a \neq 0$, then $b/a=b\cdot a^{-1}$.

T10. If $a \neq 0$, then $(a^{-1})^{-1}=a$.

T11. *Zero Product Property* If $ab=0$, then $a=0$ or $b=0$.

T12. *Rule for Multiplication with Negative Signs*

$$(-a)b=a(-b)=-(ab), \qquad (-a)(-b)=ab,$$

and

$$-\frac{a}{b}=\frac{-a}{b}=\frac{a}{-b}.$$

T13. *Equivalent Fractions Property*

$$\frac{a}{b}=\frac{ac}{bc}, \quad \text{if } b \neq 0 \text{ and } c \neq 0.$$

T14. *Rule for Addition of Fractions*

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}, \quad \text{if } b \neq 0 \text{ and } d \neq 0.$$

T15. *Rule for Multiplication of Fractions*

$$\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}, \quad \text{if } b \neq 0 \text{ and } d \neq 0.$$

T16. *Rule for Division of Fractions*

$$\frac{\frac{a}{b}}{\frac{c}{d}}=\frac{ad}{bc}, \quad \text{if } b \neq 0,\ c \neq 0, \text{ and } d \neq 0.$$

T17. *Trichotomy Law* For arbitrary real numbers a and b, exactly one of the three relations $a < b$, $b < a$, or $a = b$ holds.

T18. *Transitive Law* If $a < b$ and $b < c$, then $a < c$.

T19. If $a < b$, then $a + c < b + c$.

T20. If $a < b$ and $c > 0$, then $ac < bc$.

T21. If $a \neq 0$, then $a^2 > 0$.

T22. $1 > 0$.

T23. If $a < b$ and $c < 0$, then $ac > bc$.

T24. If $a < b$, then $-a > -b$. In particular, if $a < 0$, then $-a > 0$.

T25. If $ab > 0$, then both a and b are positive or both are negative.

T26. If $a < c$ and $b < d$, then $a + b < c + d$.

T27. If $0 < a < c$ and $0 < b < d$, then $0 < ab < cd$.

One final axiom distinguishes the set of real numbers from the set of rational numbers. It is called the **least upper bound axiom**.

LUB. Any nonempty set S of real numbers that is bounded above has a least upper bound. That is, if B is the set of all real numbers x such that $x \geq s$ for every s in S and if B has at least one element, then B has a smallest element. This element is called the **least upper bound** of S.

The least upper bound axiom holds for the set of real numbers but not for the set of rational numbers. For example, the set of all rational numbers that are less than $\sqrt{2}$ has upper bounds but not a least upper bound within the set of rational numbers.

Chapter 6

Relation

For $(x, y) \in R$ and $R \subseteq A \times B$

$x R y$, iff $(x, y) \in R$.

Relation on a set A

A relation on set A is a relation of A x A $R \subseteq A \times A$

Domain, Co-Domain, Range

Let A and B be sets and R be a relation from A to B.

The **domain** of R, $Dom(R)$, is the set $\{a \in A : aRb \text{ for some } b \in B\}$.

(i.e. values of A)

The **co-domain** of R, $coDom(R)$, is the set B.

(i.e. ***all*** values of B)

The **range** of R, $Range(R)$, is the set $\{b \in B : aRb \text{ for some } a \in A\}$.

(i.e. values of B st aRb)

Inverse Relation

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

$$\forall x \in A, \forall y \in B \left((y, x) \in R^{-1} \Leftrightarrow (x, y) \in R\right).$$

Composition

Let A, B and C be sets. Let $R \subseteq A \times B$ be a relation. Let $S \subseteq B \times C$ be a relation. The **composition of** R **with** S, denoted $S \circ R$, is the relation from A to C such that:

$$\forall x \in A, \forall z \in C \left(x \, S \circ R \, z \Leftrightarrow \left(\exists y \in B \; (xRy \wedge ySz)\right)\right)$$

Note that $S \circ R$ means R is applied first, then S

Proposition: Composition is associative

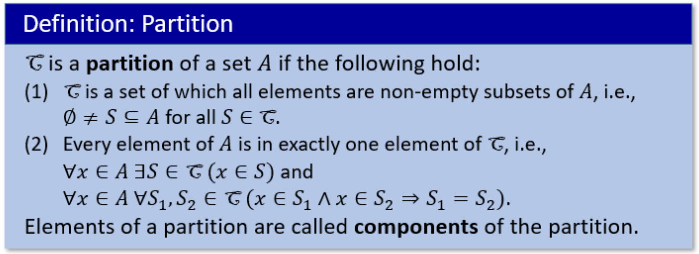
$$T \circ (S \circ R) = (T \circ S) \circ R = T \circ S \circ R$$

Proposition: Inverse of Composition

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

n-ary relation

is a subset of a n-tuple



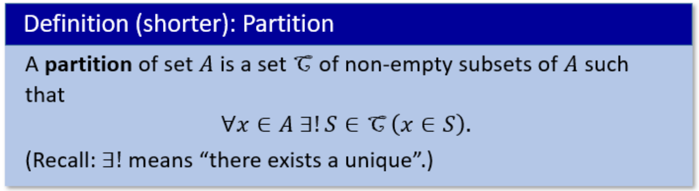
Definition: Partition

$\mathcal{C}$ is a **partition** of a set A if the following hold:

(1) $\mathcal{C}$ is a set of which all elements are non-empty subsets of A, i.e., $\emptyset \neq S \subseteq A$ for all $S \in \mathcal{C}$.

(2) Every element of A is in exactly one element of $\mathcal{C}$, i.e., $\forall x \in A \, \exists S \in \mathcal{C} \, (x \in S)$ and $\forall x \in A \, \forall S_1, S_2 \in \mathcal{C} \, (x \in S_1 \wedge x \in S_2 \Rightarrow S_1 = S_2)$.

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



Definition (shorter): Partition

A **partition** of set A is a set $\mathcal{C}$ of non-empty subsets of A such that

$$\forall x \in A \, \exists! \, S \in \mathcal{C} \, (x \in S).$$

(Recall: ∃! means "there exists a unique".)

The first one states that every element is in a component

The second one states that if an element is in two components, both components are the same

Definition: Relation Induced by a Partition

Given a partition C of a set A, the relation R **induced by the partition** is defined on A as follows:

$\forall x, y \in A, xRy \Leftrightarrow \exists$ a component S of C s.t. $x, y \in S$.

Theorem 8.3.1 Relation Induced by a Partition

Let A be a set with a partition and let R be the relation induced by the partition. Then R is reflexive, symmetric, and transitive.

Definition: Equivalence Relation

Let A be a set and R a relation on A. R is an **equivalence relation** iff R is reflexive, symmetric and transitive.

Theorem 8.3.4 The Partition Induced by an Equivalence Relation

If A is a set and R is an equivalence relation on A, then the distinct equivalence classes of R form a partition of A; that is, the union of the equivalence classes is all of A, and the intersection of any two distinct classes is empty.

Definition: Equivalence Class

Suppose A is a set and $\sim$ is an equivalence relation on A. For each $a \in A$, the **equivalence class** of a, denoted $[\boldsymbol{a}]$ and called the **class of $\boldsymbol{a}$** for short, is the set of all elements $x \in A$ s.t. a is $\sim$-related to x.

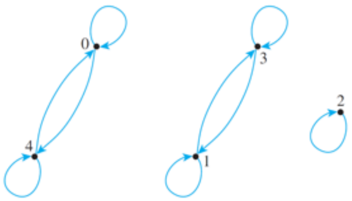
An equivalence class [x]~ is the set of all values y, such that x~y
[(4,3)] is the set of all values (a,b) such that (4~3)~(a,b)
So the equivalence class is just a set of values. Not the relation itself
[1] is the set of all values (x) such that 1~x

Symbolically,

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

Or: $\forall x \in A\ (x \in [a]_\sim \Leftrightarrow a \sim x)$.

First find the equivalence class of every element of A.



$$[0] = \{x \in A : 0\ R\ x\} = \{0,4\}$$
$$[1] = \{x \in A : 1\ R\ x\} = \{1,3\}$$
$$[2] = \{x \in A : 2\ R\ x\} = \{2\}$$
$$[3] = \{x \in A : 3\ R\ x\} = \{1,3\}$$
$$[4] = \{x \in A : 4\ R\ x\} = \{0,4\}$$

Note that [0] = [4] and [1] = [3]. Thus the *distinct* equivalence classes of the relation are {0, 4}, {1, 3}, and {2}.

Lemma Rel.1 Equivalence Classes

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) $[x] \cap [y] \neq \emptyset$.

We prove this by proving:

$$\begin{tikzcd} & \text{(i)} \arrow[dr, Rightarrow] & \\ \text{(iii)} \arrow[ur, Rightarrow] & & \text{(ii)} \arrow[ll, Rightarrow] \end{tikzcd}$$

Proof

If [x1], [x2] in A/~
Then x1~x2

Definition:
$[a]_\sim = \{x \in A : a \sim x\}$

1. ((i) ⇒ (ii))
   1.1. Suppose $x \sim y$.
   1.2. Then $y \sim x$ — by symmetry.
   1.3. For every $z \in [x]$,
      1.3.1. $x \sim z$ — by the definition of $[x]$;
      1.3.2. $\therefore y \sim z$ — by transitivity, as $y \sim x$;
      1.3.3. $\therefore z \in [y]$ — by the definition of $[y]$.
   1.4. This shows $[x] \subseteq [y]$.
   1.5. Switching the roles of x and y, we see also that $[y] \subseteq [x]$.
   1.6. Therefore, $[x] = [y]$.

If you follow the definition you should be writing
1.3.1 z~x (by defn of [x])
1.3.2 x~z (by transitivity)

Proof

Definition:
$[a]_\sim = \{x \in A : a \sim x\}$

2. ((ii) ⇒ (iii))
   2.1. Suppose $[x] = [y]$.
   2.2. Then $[x] \cap [y] = [x]$ — by the Idempotent Law for ∩.
   2.3. However, we know $x \sim x$ — by the reflexivity of ~.
   2.4. This shows $x \in [x] = [x] \cap [y]$ — by the definition of [x] and line 2.2.
   2.5. Therefore, $[x] \cap [y] \neq \emptyset$.

Proof

Definition:
$[a]_\sim = \{x \in A : a \sim x\}$

3. ((iii) ⇒ (i))
   3.1. Suppose $[x] \cap [y] \neq \emptyset$.
   3.2. Take $z \in [x] \cap [y]$.
   3.3. Then $z \in [x]$ and $z \in [y]$ — by the definition of ∩.
   3.4. Then $x \sim z$ and $y \sim z$. — by the definition of $[x]$ and $[y]$.
   3.5. $y \sim z$ implies $z \sim y$ — by symmetry.
   3.6. Therefore, $x \sim y$ — by transitivity.

Congruence

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. Then a is congruent to b modulo n iff $\boldsymbol{a - b = nk}$ for some $k \in \mathbb{Z}$. In other words, $\boldsymbol{n} \mid (\boldsymbol{a - b})$.

In this case, we write $\boldsymbol{a \equiv b\ (\mathbf{mod}\ n)}$.

Proposition

Congruence-mod n is an equivalence relation on $\mathbb{Z}$ for every $n \in \mathbb{Z}^+$.

Proof:

1. (Reflexivity) For all $a \in \mathbb{Z}$,
   - 1.1. $a - a = 0 = n \times 0$.
   - 1.2. So $a \equiv a\ (\text{mod}\ n)$ by the defn of congruence.
2. (Symmetry)
   - 2.1. Let $a, b \in \mathbb{Z}$ such that $a \equiv b\ (\text{mod}\ n)$.
   - 2.2. Then there is a $k \in \mathbb{Z}$ such that $a - b = nk$.
   - 2.3. Then $b - a = -(a - b) = -nk = n(-k)$.
   - 2.4. $-k \in \mathbb{Z}$ (by closure of integers under ×), so $b \equiv a\ (\text{mod}\ n)$ by the definition of congruence.
3. (Transitivity)
   - 3.1. Let $a, b, c \in \mathbb{Z}$ such that $a \equiv b\ (\text{mod}\ n)$ and $b \equiv c\ (\text{mod}\ n)$.
   - 3.2. Then there are $k, l \in \mathbb{Z}$ such that $a - b = nk$ and $b - c = nl$.
   - 3.3. Then $a - c = (a - b) + (b - c) = nk + nl = n(k + l)$.
   - 3.4. $k + l \in \mathbb{Z}$ (by closure of integers under $+$), so $a \equiv c\ (\text{mod}\ n)$ by the definition of congruence.

A relation R on a set A is

reflexive: $\forall x \in A\ (x\ R\ x)$;

symmetric:

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

transitive:

$\forall x, y, z \in A$

$(x\ R\ y \wedge y\ R\ z \Rightarrow x\ R\ z)$.

Revisit Example #12:

Define a relation R on $\mathbb{Z}$ as follows:

$$\forall x, y \in \mathbb{Z}\ (x\ R\ y\ \Leftrightarrow 3 \mid (x - y)).$$

This relation is called congruence modulo 3.

It has been shown that R is an equivalence relation.

What are the distinct equivalence classes of R?

The distinct equivalent classes of R are:

- $\{3k : k \in \mathbb{Z}\}$, {…,-9,-6,-3,0,3,6,9,…}
- $\{3k + 1 : k \in \mathbb{Z}\}$, and {…,-8,-5,-2,1,4,7,10,…}
- $\{3k + 2 : k \in \mathbb{Z}\}$. {…,-7,-4,-1,2,5,8,11,…}

Observe that {{…,-9,-6,-3,0,3,6,9,…}, {…,-8,-5,-2,1,4,7,10,…}, {…,-7,-4,-1,2,5,8,11,…}} is a partition of $\mathbb{Z}$.

Definition: Equivalence Class

Suppose A is a set and $\sim$ is an equivalence relation on A. The **equivalence class** of $a \in A$, is $[a]_\sim = \{x \in A : a \sim x\}$.

Congruence: Equivalence classes

Let $n \in \mathbb{Z}^+$. The equivalence classes w.r.t. the congruence-mod-n relation on are of the form:

$$\begin{aligned}[x] &= \{y \in \mathbb{Z} : x \equiv y\ (\text{mod}\ n)\}\\ &= \{y \in \mathbb{Z} : x - y = nk \text{ for some } k \in \mathbb{Z}\}\\ &= \{x + nk : k \in \mathbb{Z}\}\\ &= \{\dots, x - 2n, x - n, x, x + n, x + 2n, \dots\} \text{ where } x \in \mathbb{Z}.\end{aligned}$$

Note that for all $x \in \mathbb{Z}$, $[x + n] = \{\dots, x - n, x, x + n, x + 2n, x + 3n, \dots\} = [x]$.

Congruence modulo 4

:	:	:	:
-8	-7	-6	-5
-4	-3	-2	-1
0	1	2	3
4	5	6	7
8	9	10	11
:	:	:	:

$\mathbb{Z}$

For example, if $n = 4$, then

$\cdots = [-8] = [-4] = [0] = [4] = \cdots$ and $\cdots = [-7] = [-3] = [1] = [5] = \cdots$

and so on.

Definition: Set of equivalence classes

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 $\sim$”.

Example #18: Let $n \in \mathbb{Z}^+$. If $\sim_n$ denotes the congruence-mod-n relation on $\mathbb{Z}$, then

$$\begin{aligned}\mathbb{Z}/\sim_n &= \{[x] : x \in \mathbb{Z}\}\\ &= \{\{nk : k \in \mathbb{Z}\}, \{nk+1 : k \in \mathbb{Z}\}, \cdots, \{nk+(n-1) : k \in \mathbb{Z}\}\}.\end{aligned}$$

Theorem Rel.2 Equivalence classes form a partition

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

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

$\mathcal{C}$ is a **partition** of a set A if:

(1) $\mathcal{C}$ is a set of which all elements are nonempty subsets of A.

(2) Every element of A is in exactly one element of $\mathcal{C}$.

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. $x \sim x$ by the reflexivity of $\sim$.
   - 2.5. Hence $x \in [x] = S$ by the definition 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. $x \sim x$ by the reflexivity of $\sim$.
   - 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. $x \in [y_1] \cap [y_2]$ by lines 4.1 and 4.2.
   - 4.4. So $[y_1] \cap [y_2] \neq \emptyset$.
   - 4.5. Therefore $S_1 = [y_1] = [y_2] = S_2$ by lemma: equivalence classes.

Lemma Rel.1 Equivalence Classes

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) $[x] \cap [y] \neq \emptyset$.

Definition: Partial Order Relation

Let R be a relation on a set A. Then R is a **partial order relation** (or simply **partial order**) iff R is reflexive, antisymmetric and transitive.

Definition: Partially Ordered Set

A set A is called a **partially ordered set** (or **poset**) with respect to a partial order relation R on A, denoted by (A, R).

Definition: Comparability

Suppose $\preccurlyeq$ is a partial order relation on a set A. Elements a and b of A are said to be **comparable** iff either $a \preccurlyeq b$ or $b \preccurlyeq a$. Otherwise, a and b are **noncomparable**.

Let a set A be partially ordered with respect to a relation $\preccurlyeq$ and $c \in A$.

Proposition: A smallest element is minimal.

Consider a partial order $\preccurlyeq$ on a set A. Any smallest element is minimal.

Definition: Total Order Relations

If R is a partial order relation on a set A, and for any two elements x and y in A, either $x\,R\,y$ or $y\,R\,x$, then R is a **total order relation** (or simply **total order**) on A.

In other words, R is a total order iff

R is a partial order and
$\forall x, y \in A\ (x\,R\,y\ \vee y\,R\,x)$.

Definition: Linearization of a partial order

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

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

Definition: Well-Ordered Set

Let $\preccurlyeq$ be a **total order** on a set A. A is **well-ordered** iff every non-empty subset of A contains a smallest element. Symbolically,

$$\forall S \in \mathcal{P}(A),\ S \neq \emptyset \Rightarrow \big(\exists x \in S\ \forall y \in S\ (x \preccurlyeq y)\big).$$

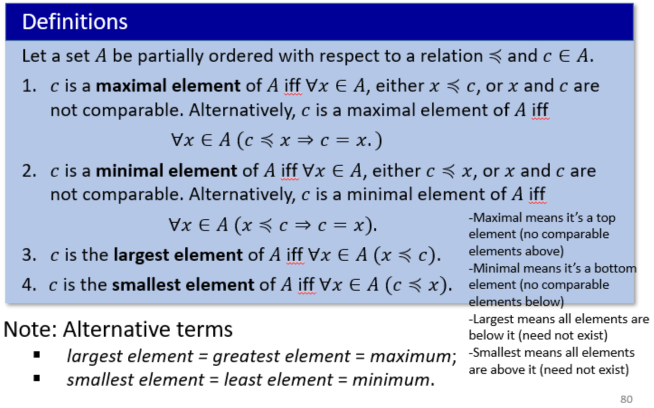
Notes:

$[a]_\sim = \{x \in A : a{\sim}x\}$ equivalence class
[x]~is the set of all y such that y~x

$A/{\sim} = \{[x]_\sim : x \in A\}$. Set of all equivalence classes

A partial order may have all elements non-comparable
A total ordered set must be a partial order
A well-ordered set must be a total order

Equality (=) is both a partial or equivalent relation



Definitions

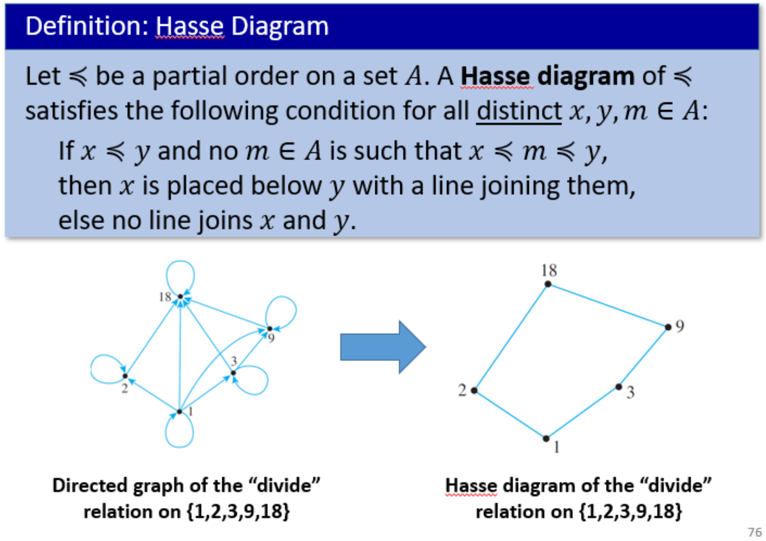
Let a set A be partially ordered with respect to a relation $\preccurlyeq$ and $c \in A$.

1. c is a **maximal element** of A iff $\forall x \in A$, either $x \preccurlyeq c$, or x and c are not comparable. Alternatively, c is a maximal element of A iff
$$\forall x \in A\ (c \preccurlyeq x \Rightarrow c = x.)$$
2. c is a **minimal element** of A iff $\forall x \in A$, either $c \preccurlyeq x$, or x and c are not comparable. Alternatively, c is a minimal element of A iff
$$\forall x \in A\ (x \preccurlyeq c \Rightarrow c = x).$$
3. c is the **largest element** of A iff $\forall x \in A\ (x \preccurlyeq c)$.
4. c is the **smallest element** of A iff $\forall x \in A\ (c \preccurlyeq x)$.

-Maximal means it's a top element (no comparable elements above)
-Minimal means it's a bottom element (no comparable elements below)
-Largest means all elements are below it (need not exist)
-Smallest means all elements are above it (need not exist)

Note: Alternative terms

- *largest element = greatest element = maximum;*
- *smallest element = least element = minimum.*



Definition: Hasse Diagram

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

If $x \preccurlyeq y$ and no $m \in A$ is such that $x \preccurlyeq m \preccurlyeq y$,
then x is placed below y with a line joining them,
else no line joins x and y.

Directed graph of the "divide" relation on {1,2,3,9,18}

Hasse diagram of the "divide" relation on {1,2,3,9,18}

▪ R is **transitive** iff $\forall x, y,$

1. (Reflexivity) Take any $(a, b) \in B \times B$,
   1.1. $a \leq a$ and $b \leq b$.
   1.2. So $(a, b)\ R\ (a, b)$ by the definition of R.
   1.3. Hence R is reflexive.
2. (Antisymmetry) Take any $(a, b), (c, d) \in B \times B$,
   2.1. Suppose $(a, b)\ R\ (c, d)$ and $(c, d)\ R\ (a, b)$.
   2.2. Then $a \leq c, b \leq d, c \leq a$ and $d \leq b$ by the definition of R.
   2.3. Then $a = c$ and $b = d$ by the antisymmetry of $\leq$.
   2.4. So $(a, b) = (c, d)$ by equality of ordered pairs.
   2.5. Hence R is antisymmetric.
3. (Transitivity) Take any $(a, b), (c, d), (e, f) \in B \times B$,
   3.1. Suppose $(a, b)\ R\ (c, d)$ and $(c, d)\ R\ (e, f)$.
   3.2. Then $a \leq c, b \leq d, c \leq e$ and $d \leq f$ by the definition of R.
   3.3. Then $a \leq e$ and $b \leq f$ by the transitivity of $\leq$.
   3.4. So $(a, b)\ R\ (e, f)$ by the definition of R.
   3.5. Hence R is transitive.

Reflexive $\forall x \in A\ (xRx)$ All elements loop back Note that if A is empty, it is reflexive	Not reflexive $\exists x \in A\ (x\ !\ R\ x)$ At least 1 element does not loop back (Note that if A is no empty and R is empty, R is not reflexive because there is at least one element which does not loop back)
Symmetry $\forall x, y \in A\ (xRy \Rightarrow yRx)$ All two-headed arrow	Not symmetry $\exists x, y \in A\ (xRy \land y\ !\ R\ x)$ At least 1 non-two-headed arrow
Transitivity: $\forall x, y, z \in A\ (xRy \land yRz \Rightarrow xRz)$. If $a \rightarrow b$ and b → c, $a \rightarrow c$	Not transitive $\exists x, y, z \in A\ (x\ R\ y \land y\ R\ z \land x!\ Rz)$. At least 1 element where a ↛ c
Antisymmetric: $\forall x, y \in A\ (x\ R\ y \land y\ R\ x \Rightarrow x = y)$. If xRy and yRx, x=y. (Reflexivity is possible but not a req nor a guarantee) Used in partial orders, where there is some direction to it	Not antisymmetric $\exists x, y \in A\ (x\ R\ y \land y\ R\ x \land x \neq y)$. At least 1 double headed arrow with element not being itself
Irreflexive: $\forall x \in A\ (x\ (!\ R)\ x)$. There are no loops	Not irreflexive $\exists x \in A\ (xRx)$ At least one loop
Asymmetry: $\forall x, y \in A\ (x\ R\ y \Rightarrow\ y\ (!\ R)\ x)$. If xRy, y is not R (Must be irreflexive, there are no loops)	Not asymmetry $\exists x, y \in A\ (x\ R\ y \land\ y\ R\ x)$ At least one where x R y and y Rx

Chapter 7: Functions

A function f from a set X to a set Y, denoted $f: X \to Y$, is a relation satisfying the following properties:

(F1) $\forall x \in X\ \exists y \in Y\ (x, y) \in f$.

(F2) $\forall x \in X\ \forall y_1, y_2 \in Y\ \big(((x, y_1) \in f \wedge (x, y_2) \in f) \to y_1 = y_2\big)$. (That is, the y in (F1) is unique.)

Or $\forall x \in X\ \exists!\, y \in Y\ (x, y) \in f$.

i.e. each element in the preimage only has one image

Definitions: Argument, image, preimage , input, output

Let $f: X \to Y$ be a function. We write $f(x) = y$ iff $(x, y) \in f$.

We say that "f sends/maps x to y" and we may also write $x \xrightarrow{f} y$ or $f: x \longmapsto y$. Also, x is called the **argument** of f.

$f(x)$ is read "f of x", or "the **output** of f for the **input** x", or "the value of f at x", or "the **image** of x under f".

If $f(x) = y$, then x is a **preimage** of y.

Definitions: Setwise image and preimage

Let $f: X \to Y$ be a function from set X to set Y.

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

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

Inverse function only exists in a bijective function, setwise preimage always exists. If A is a set, it is a setwise preimage. If it is an element, it is an inverse function. An image may have more than one preimage

$g^{-1}(\{0,1,2\}) = \{-1,0,1\}$. (Because $g(0) = 0$; $g(-1) = g(1) = 1$.)

Definitions: Domain, co-domain, range

Let $f: X \to Y$ be a function from set X to set Y.

- X is the **domain** of f and Y the **co-domain** of f.
- The **range** of f is the (setwise) image of X under f:

$\{y \in Y : y = f(x)$ for some $x \in X\}$.

Range ⊆ Co-domain

A function f from a set X to a set Y, denoted $f: X \to Y$, is a relation satisfying the following properties:

(F1) $\forall x \in X\ \exists y \in Y\ (x, y) \in f$.

(F2) $\forall x \in X\ \forall y_1, y_2 \in Y\ \big(((x, y_1) \in f \wedge (x, y_2) \in f) \to y_1 = y_2\big)$.
(That is, the y in (F1) is unique.)

Or $\forall x \in X\ \exists!\, y \in Y\ (x, y) \in f$.

i.e. each element in the preimage only has one image

Definitions: Argument, image, preimage , input, output

Let $f: X \to Y$ be a function. We write $f(x) = y$ iff $(x, y) \in f$.

We say that "f sends/maps x to y" and we may also write $x \xrightarrow{f} y$ or $f: x \longmapsto y$. Also, x is called the **argument** of f.

$f(x)$ is read "f of x", or "the **output** of f for the **input** x", or "the value of f at x", or "the **image** of x under f".

If $f(x) = y$, then x is a **preimage** of y.

Definitions: Setwise image and preimage

Let $f: X \to Y$ be a function from set X to set Y.

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

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

Inverse function only exists in a bijective function, setwise preimage always exists. If A is a set, it is a setwise preimage. If it is an element, it is an inverse function. An image may have more than one preimage

$g^{-1}(\{0,1,2\}) = \{-1,0,1\}$. (Because $g(0) = 0$; $g(-1) = g(1) = 1$.)

Definitions: Domain, co-domain, range

Let $f: X \to Y$ be a function from set X to set Y.

- X is the **domain** of f and Y the **co-domain** of f.
- The **range** of f is the (setwise) image of X under f:

$\{y \in Y : y = f(x)$ for some $x \in X\}$.

Range ⊆ Co-domain

Sequences

A sequence $a_0, a_1, a_2, \cdots$ can be represented by a function a whose domain is $\mathbb{Z}_{\geq 0}$ that satisfies $a(n) = a_n$ for every $n \in \mathbb{Z}_{\geq 0}$.

Fibonacci Sequence

The **Fibonacci sequence** $F_0, F_1, F_2, \cdots$ is defined by setting, for each $n \in \mathbb{Z}_{\geq 0}$, $F_0 = 0$ and $F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$.

Definition: String

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

$a_0 a_1 a_2 \cdots a_{l-1}$ where $l \in \mathbb{Z}_{\geq 0}$ and $a_0, a_1, a_2, \cdots, a_{l-1} \in A$.

Here l is called the **length** of the string. The **empty string** ε is the string of length 0.

Let A^* denote the set of all strings over A.

Definition: Equality of Sequences

Given two sequences $a_0, a_1, a_2, \cdots$ and $b_0, b_1, b_2, \cdots$ defined by the functions $a(n) = a_n$ and $b(n) = b_n$ respectively for every $n \in \mathbb{Z}_{\geq 0}$, we say that the two sequences are equal if and only if $a(n) = b(n)$ for every $n \in \mathbb{Z}_{\geq 0}$.

Definition: Equality of Strings

Given two strings $s_1 = a_0a_1a_2 \cdots a_{l-1}$ and $s_2 = b_0b_1b_2 \cdots b_{l-1}$ where $l \in \mathbb{Z}_{\geq 0}$, we say that $s_1 = s_2$ if and only if $a_i = b_i$ for all $i \in \{0,1,2,\dots,l-1\}$.

Theorem 7.1.1 Function Equality

Two functions $f: A \to B$ and $g: C \to D$ are equal, i.e. $f = g$, iff (i) $A = C$ and $B = D$, and (ii) $f(x) = g(x)\ \forall x \in A$.

Definition: Injection (one-to-one function)

A function $f: X \to Y$ is **injective** (or **one-to-one**) iff

$$\forall x_1, x_2 \in X\ (f(x_1) = f(x_2) \Rightarrow x_1 = x_2).$$

or, equivalently (contrapositive), $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$.

An injective function is called an **injection**.

A function $f: X \to Y$ is **not injective** iff

$$\exists x_1, x_2 \in X\ (f(x_1) = f(x_2) \wedge x_1 \neq x_2).$$

Definition: Surjection (onto function)

A function $f: X \to Y$ is **surjective** (or **onto**) iff

$$\forall y \in Y\ \exists x \in X\ \big(y = f(x)\big).$$

Every element in the co-domain has a preimage. So, range = co-domain.

A surjective function is called a **surjection**.

A function $f: X \to Y$ is **not surjective** iff

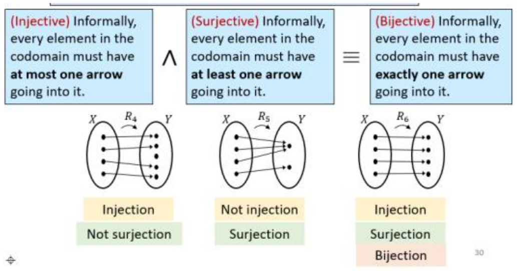
$$\exists y\ \in Y\ \forall x \in X\ \big(y \neq f(x)\big).$$

Definition: Bijection (one-to-one correspondence)

A function $f: X \to Y$ is **bije ctive** iff f is injective and surjective, i.e.

$$\forall y \in Y\ \exists!\, x \in X\ \big(y = f(x)\big).$$

A bijective function is called a **bijection** or **one-to-one correspondence**.



(Injective) Informally, every element in the codomain must have **at most one arrow** going into it. ∧ (Surjective) Informally, every element in the codomain must have **at least one arrow** going into it. ≡ (Bijective) Informally, every element in the codomain must have **exactly one arrow** going into it.

Definition: Inverse function

Let $f: X \to Y$. Then $g: Y \to X$ is an **inverse** of f iff

$$\forall x \in X\ \forall y \in Y\ \big(y = f(x) \Leftrightarrow x = g(y)\big).$$

We denote the inverse of f as f^{-1}.

Proposition: Uniqueness of inverses

If g_1 and g_2 are inverses of $f: X \to Y$, then $g_1 = g_2$.

Theorem 7.2.3

If $f: X \to Y$ is a bijection, then $f^{-1}: Y \to X$ is also a bijection.

In other words, $f: X \to Y$ is **bijective iff f has an inverse.**

Definition: Composition of Functions

Let $f: X \to Y$ and $g: Y \to Z$ be functions. Define a new function $g \circ f: X \to Z$ as follows:

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

where $g \circ f$ is read "g circle f" and $g\big(f(x)\big)$ is read "g of f of x".

The function $g \circ f$ is called the **composition** of f and g.

Identity

$id_X(x) = x$ for all $x \in X$.

(recall to check function equality, check domain, range, image

Theorem 7.3.1 Composition with an Identity Function

If f is a function from a set X to a set Y, and id_X is the identity function on X, and id_Y is the identity function on Y, then

$$f \circ id_X = f \text{ and}$$

$$id_Y \circ f = f$$

Theorem 7.3.2 Composition of a Function with Its Inverse

If $f: X \to Y$ is a bijection with inverse function $f^{-1}: Y \to X$, then

$$f^{-1} \circ f = id_X \quad \text{and} \quad f \circ f^{-1} = id_Y$$

Theorem: Associativity of Function Composition

Let $f: A \to B,\ g: B \to C$ and $h: C \to D$. Then

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

Function composition is associative.

Theorem 7.3.3

If $f: X \to Y$ and $g: Y \to Z$ are both injective, then $g \circ f$ is injective.

Theorem 7.3.4

If $f: X \to Y$ and $g: Y \to Z$ are both surjective, then $g \circ f$ is surjective.

Note: These theorems do not prove the opposite! That if composition is surjective that individual is surjective, or likewise

Tut 6 Q6:

$f: B \to C$. Suppose we have a function g with domain C such that $g \circ f$ is injective. f is injective.

Tut 6 Q7

$f: B \to C$. Suppose we have a function e with codomain B such that $f \circ e$ is surjective. f is surjective.

Congruence (Recap)

The quotient $\mathbb{Z}/{\sim_n}$ where $\sim_n$ is the congruence-mod-n relation on $\mathbb{Z}$, is denoted $\mathbb{Z}_n$.

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. Then a is congruent to b modulo n iff $a - b = nk$ for some $k \in \mathbb{Z}$. In other words, $n \mid (a - b)$. In this case, we write $a \equiv b \pmod{n}$.

Suppose A is a set and $\sim$ is an equivalence relation on A. The **equivalence class** of $a \in A$, is $[a]_\sim = \{x \in A : a{\sim}x\}$.

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.,

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

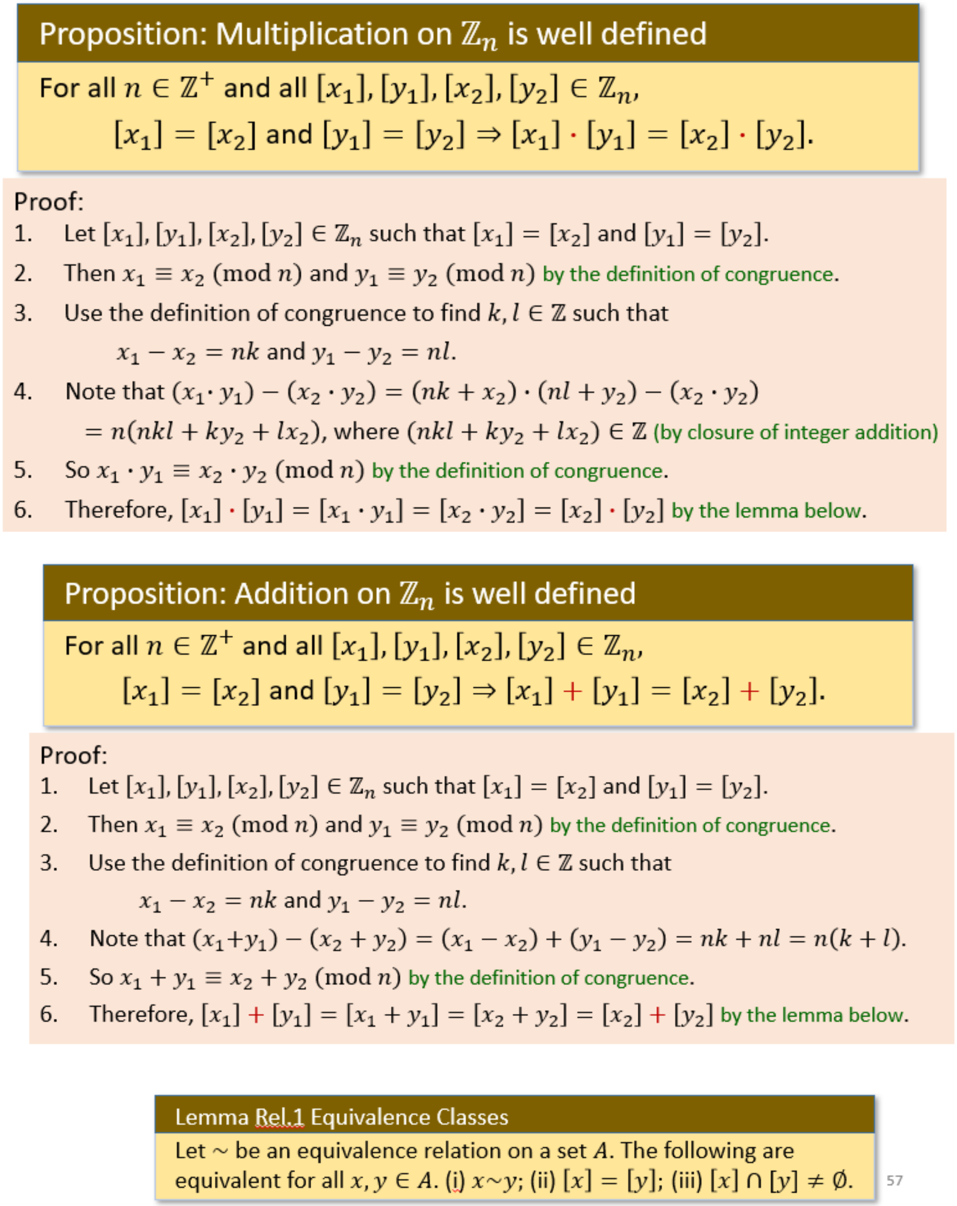
We may read $A/\sim$ as “the quotient of A by $\sim$”.

Definition: Addition and Multiplication on $\mathbb{Z}_n$

Define addition $+$ and multiplication $\cdot$ on $\mathbb{Z}_n$ as follows:

whenever $[x], [y] \in \mathbb{Z}_n$,

$[x] + [y] = [x + y]$ and $[x] \cdot [y] = [x \cdot y]$



Proposition: Multiplication on $\mathbb{Z}_n$ is well defined

For all $n \in \mathbb{Z}^+$ and all $[x_1], [y_1], [x_2], [y_2] \in \mathbb{Z}_n$,

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

Proof:

1. Let $[x_1], [y_1], [x_2], [y_2] \in \mathbb{Z}_n$ such that $[x_1] = [x_2]$ and $[y_1] = [y_2]$.
2. Then $x_1 \equiv x_2 \pmod{n}$ and $y_1 \equiv y_2 \pmod{n}$ by the definition of congruence.
3. Use the definition of congruence to find $k, l \in \mathbb{Z}$ such that
   $x_1 - x_2 = nk$ and $y_1 - y_2 = nl$.
4. Note that $(x_1 \cdot y_1) - (x_2 \cdot y_2) = (nk + x_2) \cdot (nl + y_2) - (x_2 \cdot y_2)$
   $= n(nkl + ky_2 + lx_2)$, where $(nkl + ky_2 + lx_2) \in \mathbb{Z}$ (by closure of integer addition)
5. So $x_1 \cdot y_1 \equiv x_2 \cdot y_2 \pmod{n}$ by the definition of congruence.
6. Therefore, $[x_1] \cdot [y_1] = [x_1 \cdot y_1] = [x_2 \cdot y_2] = [x_2] \cdot [y_2]$ by the lemma below.

Proposition: Addition on $\mathbb{Z}_n$ is well defined

For all $n \in \mathbb{Z}^+$ and all $[x_1], [y_1], [x_2], [y_2] \in \mathbb{Z}_n$,

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

Proof:

1. Let $[x_1], [y_1], [x_2], [y_2] \in \mathbb{Z}_n$ such that $[x_1] = [x_2]$ and $[y_1] = [y_2]$.
2. Then $x_1 \equiv x_2 \pmod{n}$ and $y_1 \equiv y_2 \pmod{n}$ by the definition of congruence.
3. Use the definition of congruence to find $k, l \in \mathbb{Z}$ such that
   $x_1 - x_2 = nk$ and $y_1 - y_2 = nl$.
4. Note that $(x_1 + y_1) - (x_2 + y_2) = (x_1 - x_2) + (y_1 - y_2) = nk + nl = n(k + l)$.
5. So $x_1 + y_1 \equiv x_2 + y_2 \pmod{n}$ by the definition of congruence.
6. Therefore, $[x_1] + [y_1] = [x_1 + y_1] = [x_2 + y_2] = [x_2] + [y_2]$ by the lemma below.

Lemma Rel.1 Equivalence Classes

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) $[x] \cap [y] \neq \emptyset$.

Chapter 8: MI

Definitions: Sequence and Terms

A **sequence** is an ordered set with members called **terms**.

Usually, the terms are numbers. A sequence may have infinite terms.

Definition: Summation

If m and n are integers, $m \leq n$, the symbol

$$\sum_{k=m}^{n} a_k$$

is the **sum** of all the terms $a_m, a_{m+1}, a_{m+2}, \cdots, a_n$.

We say that $a_m + a_{m+1} + a_{m+2} + \cdots + a_n$ is the **expanded form** of the sum, and we write

$\sum_{k=m}^{n} a_k = a_m + a_{m+1} + a_{m+2} + \cdots + a_n$.

We call k the **index** of the summation, m the **lower limit** of the summation and n the **upper limit** of the summation.

Definition: Product

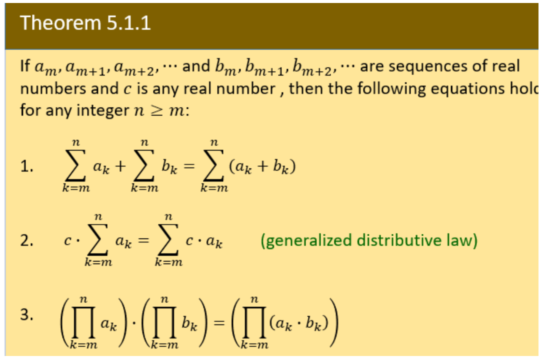
If m and n are integers, $m \leq n$, the symbol

$$\prod_{k=m}^{n} a_k$$

is the **product** of all the terms $a_m, a_{m+1}, a_{m+2}, \cdots, a_n$.

We write

$\prod_{k=m}^{n} a_k \ = a_m \cdot a_{m+1} \cdot a_{m+2} \cdot \cdots \cdot a_n$.



Theorem 5.1.1

If $a_m, a_{m+1}, a_{m+2}, \cdots$ and $b_m, b_{m+1}, b_{m+2}, \cdots$ are sequences of real numbers and c is any real number , then the following equations hold for any integer $n \geq m$:

1. $\sum_{k=m}^{n} a_k + \sum_{k=m}^{n} b_k = \sum_{k=m}^{n} (a_k + b_k)$

2. $c \cdot \sum_{k=m}^{n} a_k = \sum_{k=m}^{n} c \cdot a_k$ (generalized distributive law)

3. $\left(\prod_{k=m}^{n} a_k\right) \cdot \left(\prod_{k=m}^{n} b_k\right) = \left(\prod_{k=m}^{n} (a_k \cdot b_k)\right)$

Definition: Arithmetic Sequence

A sequence $a_0, a_1, a_2, \cdots$ is called an **arithmetic sequence** (or **arithmetic progression**) iff there is a constant d such that

$a_k \ = a_{k-1} + d$ for all integers $k \geq 1$.
If follows that,
$a_n \ = a_0 + dn$ for all integers $n \geq 0$.

Summing an arithmetic sequence of n terms:

$$\sum_{k=0}^{n-1} a_k = \frac{n}{2}(2a_0 + (n-1)d)$$

Definition: Geometric Sequence

A sequence $a_0, a_1, a_2, \cdots$ is called a **geometric sequence** (or **geometric progression**) iff there is a constant r such that

$a_k \ = r a_{k-1}$ for all integers $k \geq 1$.

If follows that,

$a_n \ = a_0 r^n$ for all integers $n \geq 0$.

Principle of Mathematical Induction (PMI)

Let $P(n)$ be a property that is defined for integers n, and let a be a fixed integer. Suppose the following 2 statements are true:

1. $P(a)$ is true.

2. For all integers $k \geq a$, if $P(k)$ is true then $P(k+1)$ is true.

Then the statement "for all integers $n \geq a$, $P(n)$" is true.

Theorem 5.2.2 (5th: 5.2.1) Sum of the First n Integers

For all integers $n \geq 1$,

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

Definition: Closed Form

If a sum with a variable number of terms is shown to be equal to a formula that does not contain either an ellipsis (…) or a summation symbol (Σ), we say that it is written in **closed form**.

Theorem 5.2.3 (5th: 5.2.2) Sum of a Geometric Sequence

For any real number $r \neq 1$, and any integers $n \geq 0$,

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

Proposition 5.3.1 (5th: 5.3.2)

For all integers $n \geq 0$, $2^{2n} - 1$ is divisible by 3.

Proposition 5.3.2 (5th: 5.3.3)

For all integers $n \geq 3$, $2n + 1 < 2^n$.

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 $a \mid c$.

Well-Ordering Principle for the Integers

Every nonempty subset of $\mathbb{Z}_{\geq 0}$ has a smallest element.

MI/1PI:
1. Let P(n) ≡ (statement is true)
2. Basis: P(1): (statement). Therefore P(1) is true
3. Assume P(k) is true for some k in range.
4. Inductive step: (show P(k+1) is true)
 4.1 P(k+1) = k/2 + k
 4.2 Therefore P(k+1) is true
5. Therefore, P(n) is true for n in range.

Note: don't pick a specific example for P(k+1), pick a generic example. Also start from P(k+1), don't start from P(k) then work backwards

Strong MI/2PI:
1. Let P(n) ≡ (statement is true)
2. Basis: P(1), P(2), P(k): (statement). Therefore P(1),P(2),P(k) is true
3. Assume P(k) is true for some k in range.
4. Inductive step: (show P(k+1) is true for every basis
 4.1 P(k+1) = k/2 + k
 4.2 Therefore P(k+1) is true
5. Therefore, P(n) is true for n in range.

Definition: Recurrence Relation

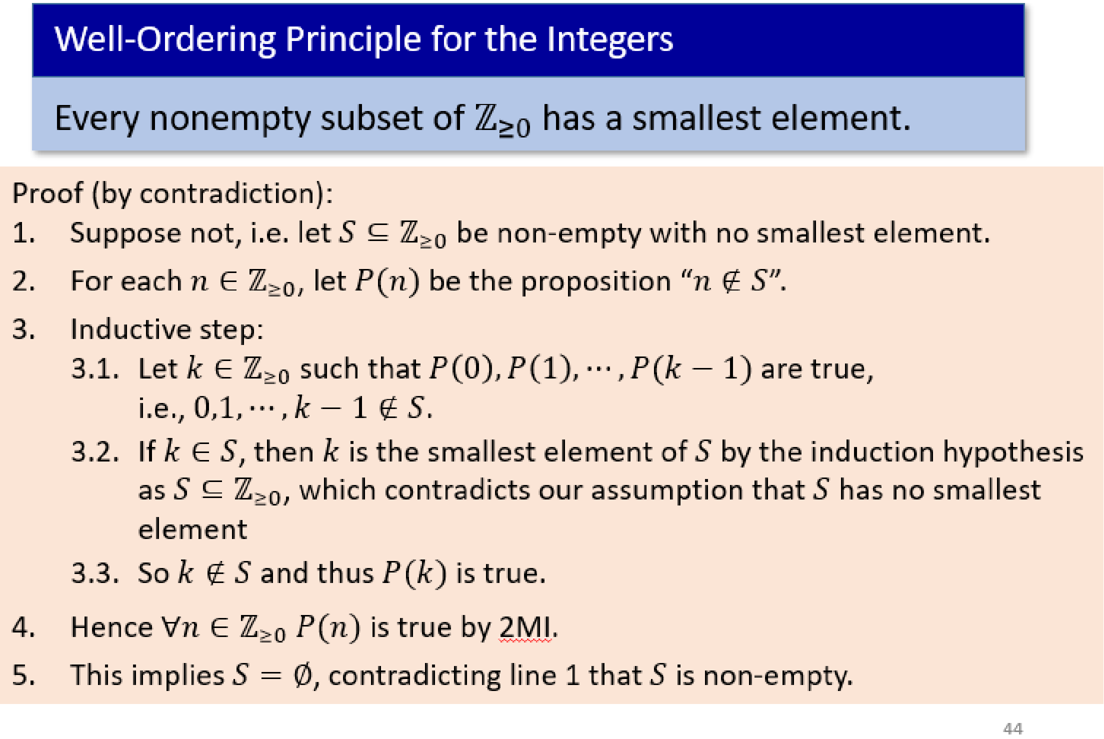
A **recurrence relation** for a sequence $a_0, a_1, a_2, \cdots$ is a formula that relates each term a_k to certain of its predecessors $a_{k-1}, a_{k-2}, \cdots, a_{k-i}$, where i is an integer with $k - i \geq 0$.

If i is a fixed integer , the **initial conditions** for such a recurrent relation specify the values of $a_0, a_1, a_2, \cdots, a_{i-1}$.

If i depends on k, the initial conditions specify the values of $a_0, a_1, a_2, \cdots, a_m$, where m is an integer with $m \geq 0$.

8.5.3. Recursively Defined Sets

Let S be a finite set with at least one element. A **string over** S is a finite sequence of elements from S. The elements of S are called **characters** of the string, and the **length** of a string is the number of characters it contains. The **null string over** S is defined to be the "string" with no characters. It is usually denoted ϵ and is said to have length 0.

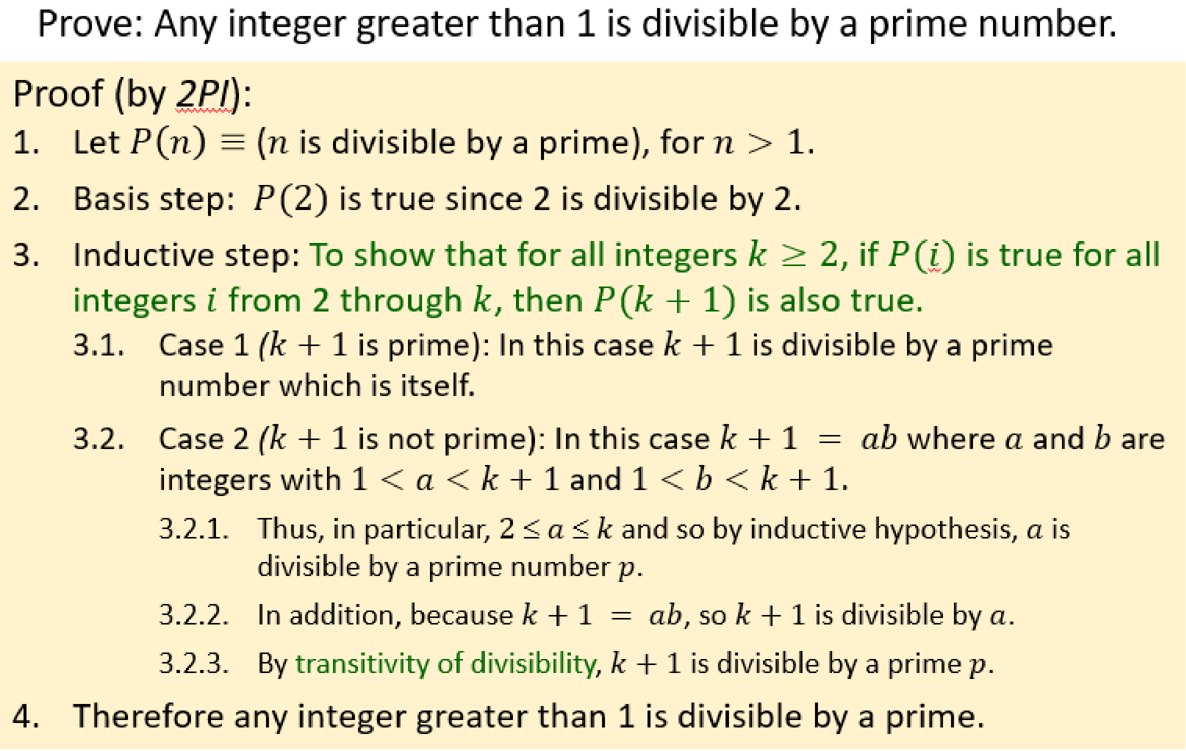


Well-Ordering Principle for the Integers

Every nonempty subset of $\mathbb{Z}_{\geq 0}$ has a smallest element.

Proof (by contradiction):

1. Suppose not, i.e. let $S \subseteq \mathbb{Z}_{\geq 0}$ be non-empty with no smallest element.
2. For each $n \in \mathbb{Z}_{\geq 0}$, let $P(n)$ be the proposition "$n \notin S$".
3. Inductive step:
   - 3.1. Let $k \in \mathbb{Z}_{\geq 0}$ such that $P(0), P(1), \cdots, P(k-1)$ are true, i.e., $0,1, \cdots, k-1 \notin S$.
   - 3.2. If $k \in S$, then k is the smallest element of S by the induction hypothesis as $S \subseteq \mathbb{Z}_{\geq 0}$, which contradicts our assumption that S has no smallest element
   - 3.3. So $k \notin S$ and thus $P(k)$ is true.
4. Hence $\forall n \in \mathbb{Z}_{\geq 0}\ P(n)$ is true by 2MI.
5. This implies $S = \emptyset$, contradicting line 1 that S is non-empty.



Prove: Any integer greater than 1 is divisible by a prime number.

Proof (by *2PI*):

1. Let $P(n) \equiv (n$ is divisible by a prime), for $n > 1$.
2. Basis step: $P(2)$ is true since 2 is divisible by 2.
3. Inductive step: To show that for all integers $k \geq 2$, if $P(i)$ is true for all integers i from 2 through k, then $P(k+1)$ is also true.
   - 3.1. Case 1 ($k+1$ is prime): In this case $k+1$ is divisible by a prime number which is itself.
   - 3.2. Case 2 ($k+1$ is not prime): In this case $k+1 = ab$ where a and b are integers with $1 < a < k+1$ and $1 < b < k+1$.
     - 3.2.1. Thus, in particular, $2 \leq a \leq k$ and so by inductive hypothesis, a is divisible by a prime number p.
     - 3.2.2. In addition, because $k+1 = ab$, so $k+1$ is divisible by a.
     - 3.2.3. By transitivity of divisibility, $k+1$ is divisible by a prime p.
4. Therefore any integer greater than 1 is divisible by a prime.

8.5.4. Structural Induction

Recursive definition of of a set S.

(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 (infinitely many) successive applications of the clauses above.

Structural induction over S.

To prove that $\forall x \in S\ P(x)$ is true, where each $P(x)$ is a proposition, it suffices to:

(basis step) show that $P(c)$ is true for every founder c; and

(induction step) show that $\forall x \in S \left(P(x) \Rightarrow P\big(f(x)\big)\right)$ 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.

Chapter 9: Cardinality

Let X and Y be sets and $f: X \to Y$ be a function.

f is **injective** iff $\forall x_1, x_2 \in X\ (f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$.

f is **surjective** iff $\forall y \in Y\ \exists x \in X\ \big(y = f(x)\big)$.

f is **bijective** iff f is injective and bijective, that is, $\forall y \in Y\ \exists!\, x \in X\ \big(y = f(x)\big)$.

$g: Y \to X$ is an inverse of f (also denoted as f^{-1}) iff
$\forall x \in X\ \forall y \in Y\ \big(y = f(x) \Leftrightarrow x = g(y)\big)$.

Theorem 7.2.3

If $f: X \to Y$ is a bijection, then $f^{-1}: Y \to X$ is also a bijection.

In other words, a function is bijective iff it has an inverse.

Pigeonhole Principle

Let A and B be finite sets. If there is an injection $f: A \to B$, then $|A| \le |B|$.

Contrapositive: Let $m, n \in \mathbb{Z}^+$ with $m > n$. If m pigeons are put into n pigeonholes, then there must be (at least) one pigeonhole with (at least) two pigeons.

Dual Pigeonhole Principle

Let A and B be finite sets. If there is a surjection $f: A \to B$, then $|A| \ge |B|$.

Contrapositive: Let $m, n \in \mathbb{Z}^+$ with $m < n$. If m pigeons are put into n pigeonholes, then there must be (at least) one pigeonhole with no pigeons.

Definitions: Finite set and Infinite set

Let $\mathbb{Z}_n = \{1,2,3,\ldots,n\}$, the set of positive integers from 1 to n.

A set S is said to be **finite** iff S is empty, or there exists a bijection from S to $\mathbb{Z}_n$ for some $n \in \mathbb{Z}^+$.

A set S is said to be **infinite** if it is not finite.

Definition: Cardinality

The **cardinality** of a finite set S, denoted $|S|$, is

(i) 0 if $S = \emptyset$, or

(ii) n if $f: S \to \mathbb{Z}_n$ is a bijection.

Theorem: Equality of Cardinality of Finite Sets

Let A and B be any finite sets.
$|A| = |B|$ iff there is a bijection $f: A \to B$.

Definition: Same Cardinality (Cantor)

Given any two sets A and B. A is said to have the **same cardinality** as B, written as $|A| = |B|$, iff there is a bijection $f: A \to B$.

The cardinality relation is an equivalence relation.

Theorem 7.4.1 Properties of Cardinality

For all sets A, B and C:

a. **Reflexive**: $|A| = |A|$.

b. **Symmetric**: $|A| = |B| \to |B| = |A|$.

c. **Transitive**: $(|A| = |B|) \wedge (|B| = |C|) \to |A| = |C|$.

The set A having the same cardinality as $\mathbb{Z}^+$ is called countably infinite.

Definition: Cardinal numbers

Define $\aleph_0 = |\mathbb{Z}^+|$. (Some author use $\mathbb{N}$ instead of $\mathbb{Z}^+$.)

$\aleph$ is pronounced "aleph", the first letter of the Hebrew alphabet. This is the first cardinal number.

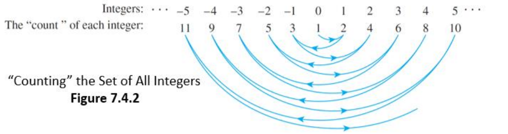
Definition: Countably infinite

A set S is said to be **countably infinite** (or, S has the cardinality of natural numbers) iff $|S| = \aleph_0$.

Definitions: Countable set and Uncountable set

A set is said to be **countable** iff it is finite or countably infinite.

A set is said to be **uncountable** if it is not countable


Integers: ⋯ −5 −4 −3 −2 −1 0 1 2 3 4 5 ⋯
The "count" of each integer: 11 9 7 5 3 1 2 4 6 8 10

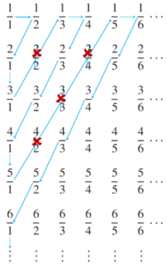
"Counting" the Set of All Integers
Figure 7.4.2

$$f(n) = \begin{cases} n/2, & \text{if } n \text{ is an even positive integer} \\ -(n-1)/2, & \text{if } n \text{ is an odd positive integer} \end{cases}$$

Example #4: Show that $\mathbb{Q}^+$ (the set of all positive rational numbers) is countable.

Display the elements of $\mathbb{Q}^+$ in a grid as shown:

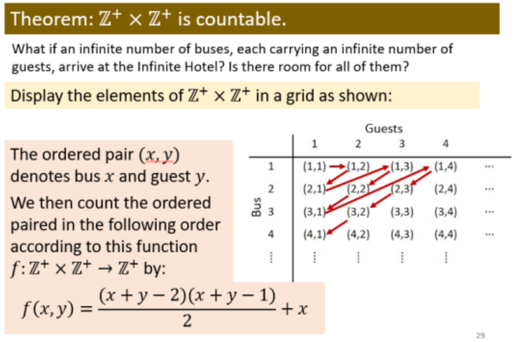
Define a function F from $\mathbb{Z}^+$ to $\mathbb{Q}^+$ by starting to count at $\frac{1}{1}$ and following the arrows as indicated, skipping over any number that has already been counted.



$\frac{1}{1}$	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{5}$	$\frac{1}{6}$	⋯
$\frac{2}{1}$	$\frac{2}{2}$	$\frac{2}{3}$	$\frac{2}{4}$	$\frac{2}{5}$	$\frac{2}{6}$	⋯
$\frac{3}{1}$	$\frac{3}{2}$	$\frac{3}{3}$	$\frac{3}{4}$	$\frac{3}{5}$	$\frac{3}{6}$	⋯
$\frac{4}{1}$	$\frac{4}{2}$	$\frac{4}{3}$	$\frac{4}{4}$	$\frac{4}{5}$	$\frac{4}{6}$	⋯
$\frac{5}{1}$	$\frac{5}{2}$	$\frac{5}{3}$	$\frac{5}{4}$	$\frac{5}{5}$	$\frac{5}{6}$	⋯
$\frac{6}{1}$	$\frac{6}{2}$	$\frac{6}{3}$	$\frac{6}{4}$	$\frac{6}{5}$	$\frac{6}{6}$	⋯
⋮	⋮	⋮	⋮	⋮	⋮	

Note:

To make countably infinite space in countably infinite set, use 2^a for element in A.



Theorem: $\mathbb{Z}^+ \times \mathbb{Z}^+$ is countable.

What if an infinite number of buses, each carrying an infinite number of guests, arrive at the Infinite Hotel? Is there room for all of them?

Display the elements of $\mathbb{Z}^+ \times \mathbb{Z}^+$ in a grid as shown:

The ordered pair (x, y) denotes bus x and guest y.

We then count the ordered paired in the following order according to this function $f: \mathbb{Z}^+ \times \mathbb{Z}^+ \to \mathbb{Z}^+$ by:

$$f(x,y) = \frac{(x+y-2)(x+y-1)}{2} + x$$

Bus \ Guests	1	2	3	4	
1	(1,1)	(1,2)	(1,3)	(1,4)	⋯
2	(2,1)	(2,2)	(2,3)	(2,4)	⋯
3	(3,1)	(3,2)	(3,3)	(3,4)	⋯
4	(4,1)	(4,2)	(4,3)	(4,4)	⋯
⋮	⋮	⋮	⋮	⋮	

29

Theorem (Cartesian Product)

If sets A and B are both countably infinite, then so is $A \times B$.

Corollary (General Cartesian Product)

Given $n \ge 2$ countably infinite sets $A_1, A_2, \cdots, A_n$, the Cartesian product $A_1 \times A_2 \times \cdots \times A_n$ is also countably infinite.

Theorem (Unions)

The union of countably many countable sets is countable. That is, if $A_1, A_2, \cdots$ are all countable sets, then so is $\bigcup_{i=1}^{\infty} A_i$

Proposition 9.1

An infinite set B is countable if and only if there is a sequence $b_0, b_1, b_2, \cdots \in B$ in which every element of B appears **exactly once.**

Lemma 9.2: Countability via Sequence

An infinite set B is countable if and only if there is a sequence $b_0, b_1, b_2, \cdots$ in which every element of B appears.

Theorem 7.4.2 (Cantor)

The set of real numbers between 0 and 1,

$$(0,1) = \{x \in \mathbb{R} \mid 0 < x < 1\}$$

is uncountable.

Theorem 7.4.3

Any subset of any countable set is countable.

Corollary 7.4.4 (Contrapositive of Theorem 7.4.3)

Any set with an uncountable subset is uncountable.

Proposition 9.3

Every infinite set has a countably infinite subset.

Lemma 9.4: Union of Countably Infinite Sets.

Let A and B be countably infinite sets. Then $A \cup B$ is countable.

Example 5

$|\mathbb{R}| = |(0,1)|$.

Tut 8

Q2: Countably infinite ∪ finite is countable

Q3a: Finite union of finite sets is finite

Q3b: Infinite union of finite sets is not finite

Q4(a) Finite union of countable sets is countable

+ Finite ∪ Finite is finite

Q5: countably infinite union of countably infinite sets is countable

Q6: |B ∪ finite| = |B|, where B is countable or uncountable

Q7: B is infinite iff there is $A \subsetneq B$ such that $|A|$ = $|B|$.

Q8: Set of complex numbers is uncountable

Q9: P(A) is uncountable for countably infinite A

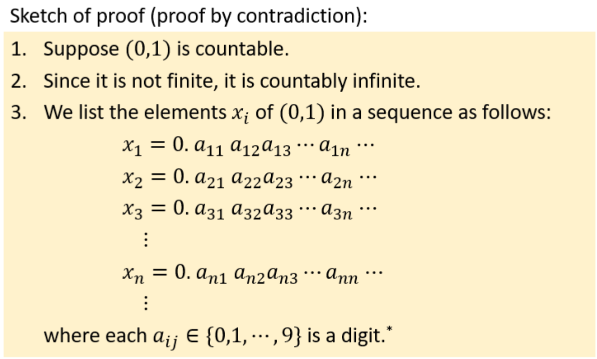
Assignment 2 Q4:

Any subset of a finite set is finite

Contrapositive: any set with an infinite subset is infinite

(a) Countably infinite \ finite is countably infinite

(c) $A \subseteq B \subseteq C$, if A and C are countably infinite, B is countably infinite

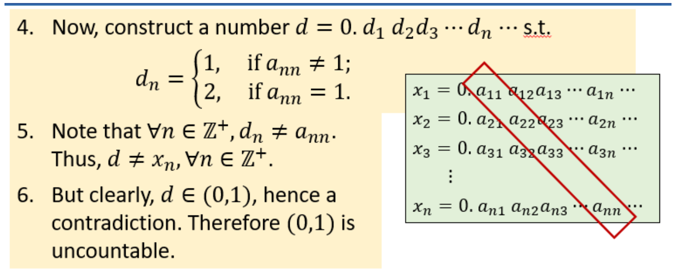


Sketch of proof (proof by contradiction):

1. Suppose (0,1) is countable.
2. Since it is not finite, it is countably infinite.
3. We list the elements x_i of $(0,1)$ in a sequence as follows:

$$x_1 = 0.\,a_{11}\,a_{12}a_{13}\cdots a_{1n}\cdots$$
$$x_2 = 0.\,a_{21}\,a_{22}a_{23}\cdots a_{2n}\cdots$$
$$x_3 = 0.\,a_{31}\,a_{32}a_{33}\cdots a_{3n}\cdots$$
$$\vdots$$
$$x_n = 0.\,a_{n1}\,a_{n2}a_{n3}\cdots a_{nn}\cdots$$
$$\vdots$$

where each $a_{ij} \in \{0,1,\cdots,9\}$ is a digit.*

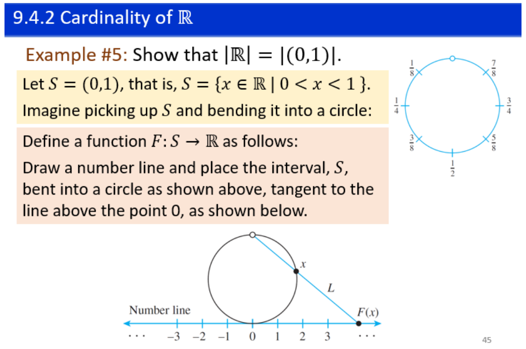


4. Now, construct a number $d = 0.\,d_1\,d_2d_3\cdots d_n\cdots$ s.t.

$$d_n = \begin{cases} 1, & \text{if } a_{nn} \neq 1; \\ 2, & \text{if } a_{nn} = 1. \end{cases}$$

5. Note that $\forall n \in \mathbb{Z}^+, d_n \neq a_{nn}$. Thus, $d \neq x_n, \forall n \in \mathbb{Z}^+$.
6. But clearly, $d \in (0,1)$, hence a contradiction. Therefore (0,1) is uncountable.

$$x_1 = 0.\,a_{11}\,a_{12}a_{13}\cdots a_{1n}\cdots$$
$$x_2 = 0.\,a_{21}\,a_{22}a_{23}\cdots a_{2n}\cdots$$
$$x_3 = 0.\,a_{31}\,a_{32}a_{33}\cdots a_{3n}\cdots$$
$$\vdots$$
$$x_n = 0.\,a_{n1}\,a_{n2}a_{n3}\cdots a_{nn}\cdots$$



9.4.2 Cardinality of $\mathbb{R}$

Example #5: Show that $|\mathbb{R}| = |(0,1)|$.

Let $S = (0,1)$, that is, $S = \{x \in \mathbb{R} \mid 0 < x < 1\}$.

Imagine picking up S and bending it into a circle:

Define a function $F: S \to \mathbb{R}$ as follows:

Draw a number line and place the interval, S, bent into a circle as shown above, tangent to the line above the point 0, as shown below.

Chapter 10 & 11: Counting

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.

Theorem 9.1.1 The Number of Elements in a List

If *m* and *n* are integers and $m \leq n$, then there are $n - m + 1$ integers from *m* to *n* inclusive.

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 $\boldsymbol{n_1 \times n_2 \times n_3 \times \ldots \times n_k}$ ways.

Theorem 5.2.4 (Sets)

Suppose A is a finite set. Then $|\mathcal{P}(A)| = 2^{|A|}$.

Theorem 9.2.2 Permutations

The number of permutations of a set with *n* ($n \geq 1$) elements is ***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 ***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
$P(n, r) = n(n - 1)(n - 2) \ldots (n - r + 1)$
$P(n, r) = n! / (n - r)!$

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
$|A \setminus B| = |A| - |B|$.

Complement

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

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

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, $n \leq km$.

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.

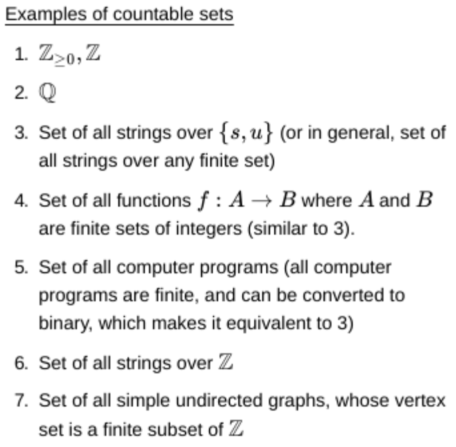
Other symbols used are $C(n, r)$, ${}_nC_r$, $C_{n,r}$, or ${}^nC_r$.

- $\binom{n}{r} = \binom{n}{n-r}$
- $k \cdot \binom{n}{k} = n \cdot \binom{n-1}{k-1}$
- $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n$

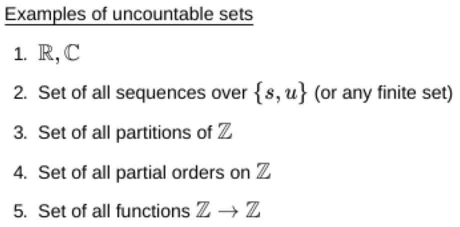
Tut 10 Q6

In P(A x A), each element is a subset of A x A.
Probability of choosing a reflexive relation is $\frac{2^{n^2-n}}{2^{n^2}} = \frac{1}{2^n}$

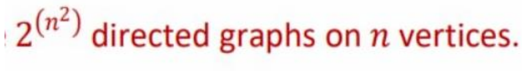
Probability of choosing a symmetric relation is $\frac{2^{\frac{n^2+n}{2}}}{2^{n^2}} = \frac{1}{2^{\frac{n^2-n}{2}}}$

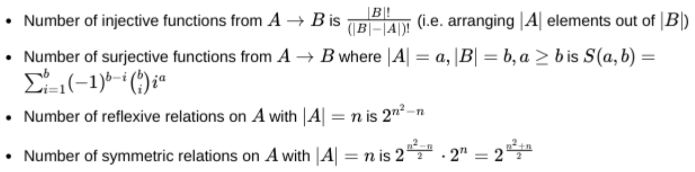

Examples of countable sets

1. $\mathbb{Z}_{\geq 0}, \mathbb{Z}$
2. $\mathbb{Q}$
3. Set of all strings over $\{s, u\}$ (or in general, set of all strings over any finite set)
4. Set of all functions $f : A \to B$ where A and B are finite sets of integers (similar to 3).
5. Set of all computer programs (all computer programs are finite, and can be converted to binary, which makes it equivalent to 3)
6. Set of all strings over $\mathbb{Z}$
7. Set of all simple undirected graphs, whose vertex set is a finite subset of $\mathbb{Z}$


Examples of uncountable sets

1. $\mathbb{R}, \mathbb{C}$
2. Set of all sequences over $\{s, u\}$ (or any finite set)
3. Set of all partitions of $\mathbb{Z}$
4. Set of all partial orders on $\mathbb{Z}$
5. Set of all functions $\mathbb{Z} \to \mathbb{Z}$


$2^{(n^2)}$ directed graphs on n vertices.


- Number of injective functions from $A \to B$ is $\frac{|B|!}{(|B|-|A|)!}$ (i.e. arranging $|A|$ elements out of $|B|$)
- Number of surjective functions from $A \to B$ where $|A| = a, |B| = b, a \geq b$ is $S(a, b) = \sum_{i=1}^{b} (-1)^{b-i} \binom{b}{i} i^a$
- Number of reflexive relations on A with $|A| = n$ is 2^{n^2-n}
- Number of symmetric relations on A with $|A| = n$ is $2^{\frac{n^2-n}{2}} \cdot 2^n = 2^{\frac{n^2+n}{2}}$

A^B is uncountable where B is countable
There are countable subsets of Z of cardinality <5

14. Which of the following sets is/are countable?

A. The set of all partitions of $\mathbb{Z}$.

B. The set of all partial orders on $\mathbb{Z}$.

C. The set of all functions $\mathbb{Z} \to \mathbb{Z}$.

D. The set $\mathbb{Z}^*$ of all strings over $\mathbb{Z}$.

E. The set of all simple undirected graphs whose vertex set is a finite subset of $\mathbb{Z}$.

Answer: D, E.

A. Each nonempty subset $S \subseteq \mathbb{Z}$ gives rise to a partition $\mathcal{C}_S = \{S\} \cup \{\{x\} : x \in \mathbb{Z} \setminus S\}$ of $\mathbb{Z}$. In this sense, different subsets of $\mathbb{Z}$ of cardinality at least 2 give rise to different partitions of $\mathbb{Z}$. From Theorem 10.4.3 and Exercise 10.4.4(5), we know there are uncountably many subsets of $\mathbb{Z}$ but only countably many of them have cardinality less than 2. So there must be uncountably many partitions of $\mathbb{Z}$ by Proposition 10.3.5.

B. Each $S \subseteq \mathbb{Z}$ gives rise to a partial order $\preccurlyeq_S$ on $\mathbb{Z}$ satisfying, for all $x, y \in \mathbb{Z}$,

$$x \preccurlyeq_S y \quad \Leftrightarrow \quad x = y \vee (x \in S \wedge y \notin S).$$

In this sense, different nonempty proper subsets of $\mathbb{Z}$ give rise to different partial orders on $\mathbb{Z}$. From Theorem 10.4.3, we know there are uncountably many subsets of $\mathbb{Z}$, but only 2 of them are empty or improper. So there must be uncountably many partial orders on $\mathbb{Z}$.

C. Every sequence $a_0, a_1, a_2, \ldots$ over $\{0,1\}$ gives rise to a function $f_a \colon \mathbb{Z} \to \mathbb{Z}$ satisfying

$$f_a(x) = \begin{cases} a_x, & \text{if } x \geqslant 0; \\ 2, & \text{if } x < 0. \end{cases}$$

As one can readily verify, different sequences over $\{0,1\}$ give rise to different functions $\mathbb{Z} \to \mathbb{Z}$ in this sense. From Exercise 10.4.4(7), we know there are uncountably many sequences over $\{0,1\}$. So there must be uncountably many functions $\mathbb{Z} \to \mathbb{Z}$ by Proposition 10.3.5.

D. Every string $a_0 a_1 \ldots a_{\ell-1}$ over $\mathbb{Z}$ gives rise to the string $\sigma_0 \sigma_1 \ldots \sigma_{\ell-1}$ over $\{\mathrm{s}, \mathrm{u}\}$, where

$$\sigma_i = \begin{cases} \mathrm{s}\,\overbrace{\mathrm{uuuuu}\ldots\mathrm{u}}^{a_i+1 \text{ many}}, & \text{if } a_i \geqslant 0; \\ \mathrm{ss}\,\underbrace{\mathrm{uuuuu}\ldots\mathrm{u}}_{-a_i \text{ many}}, & \text{if } a_i < 0. \end{cases}$$

Note that different strings over $\mathbb{Z}$ give rise to different strings over $\{\mathrm{s}, \mathrm{u}\}$ in this sense. From Exercise 10.4.4(6), we know there are countably many strings over $\{\mathrm{s}, \mathrm{u}\}$. So there must be countably many strings over $\mathbb{Z}$ by Proposition 10.3.5.

E. If G is a simple undirected graph whose vertex set V_G is a finite subset of $\mathbb{Z}$, then we can identify its edge set E_G as a subset of the finite subsets of $\mathbb{Z}$. There are countably many choices for V_G and countably many choices for E_G by Exercise 10.4.4(5). So altogether there are countably many choices by Tutorial 8 Question 5.

Definition: *r*-combination

Let *n* and *r* be non-negative integers with $r \le n$.

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

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

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

$$\binom{n}{r} = \binom{n}{n-r}$$

or, equivalently,

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

where *n* and *r* are non-negative integers with $r \le n$.

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n$$

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

$$\binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\cdots\binom{n-n_1-n_2-\cdots-n_{k-1}}{n_k} = \frac{n!}{n_1!n_2!n_3!\cdots n_k!}$$

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.

Theorem 9.7.1 Pascal's Formula

Let *n* and *r* be positive integers, $r \le n$. Then

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$$

Theorem 9.7.2 Binomial Theorem

Given any real numbers *a* and *b* and any non-negative integer *n*,

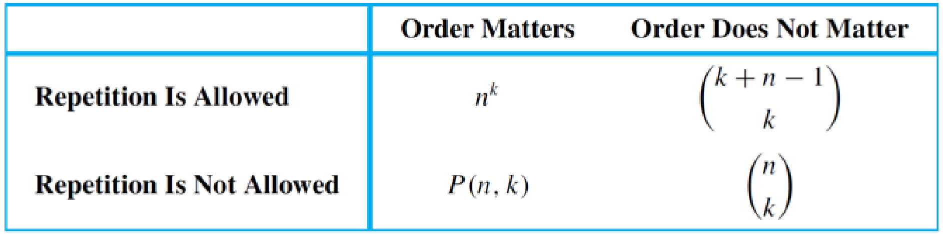
$$(a+b)^n = \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k$$
$$= a^n + \binom{n}{1}a^{n-1}b^1 + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n-1}a^1b^{n-1} + b^n$$

Theorem 6.3.1 Number of elements in a Power Set

If a set *X* has *n* ($n \ge 0$) elements, then $\mathcal{P}(X)$ has 2^n elements.

In a circle: (n-1)!

K objects to be selected from n elements, repetition allowed



	Order Matters	Order Does Not Matter
Repetition Is Allowed	n^k	$\binom{k+n-1}{k}$
Repetition Is Not Allowed	$P(n, k)$	$\binom{n}{k}$

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. $0 \leq P(A) \leq 1$
2. $P(\emptyset) = 0$ and $P(S) = 1$
3. If A and B are disjoint ($A \cap B = \emptyset$), 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

$$P(A \cup B) = P(A) + P(B) - P(A \cap B).$$

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

$$P(A|B) = \frac{P(A)P(B|A)}{P(B)}$$

$$P(B|A) = \frac{P(A \cap B)}{P(A)} \quad 9.9.1$$

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

$$P(A \cap B) = P(B|A) \cdot P(A) \quad 9.9.2$$

$$P(A) = \frac{P(A \cap B)}{P(B|A)} \quad 9.9.3$$

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

$$P(B_k|A) = \frac{P(A|B_k) \cdot P(B_k)}{P(A|B_1) \cdot P(B_1) + P(A|B_2) \cdot P(B_2) + \cdots + P(A|B_n) \cdot P(B_n)}$$

The numerator is $P(B_k \cap A) = P(A \cap Bk)$

The denominator is $P(A) = P(A \cap B_1) + P(A \cap B_2) + \cdots + P(A \cap Bn)$

Where all probabilities B_i are mutually disjoint

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 $c_1, c_2, \cdots, c_n$,

$$E\left[\sum_{i=1}^{n} c_i \cdot X_i\right] = \sum_{i=1}^{n} (c_i \cdot E[X_i])$$

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. $P(A \cap B \cap C) = P(A) \cdot P(B) \cdot P(C)$

Chapter 12 13: Graphs and Trees

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*.

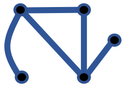
Definition: Directed Graph

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**.

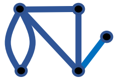
We write *e* = (*v*, *w*) for a directed edge *e* from vertex v to vertex w.

Definition: Simple Graph

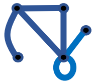
A **simple graph** is an undirected graph that does not have any loops or parallel edges. (That is, there is at most one edge between each pair of distinct vertices.)



Simple

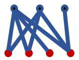


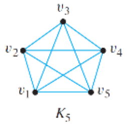
Nonsimple



Nonsimple

A **complete graph** on ***n*** **vertices**, *n* > 0, denoted $\boldsymbol{K_n}$, is a simple graph with *n* vertices and exactly one edge connecting each pair of distinct vertices.





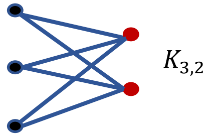
Definition: Bipartite Graph

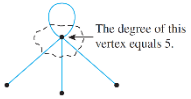
A **bipartite graph** (or bigraph) is a simple graph whose vertices can be divided into two disjoint sets U and V such that every edge connects a vertex in U to one in V.

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 $K_{m,n}$.





Definition: Subgraph of a Graph

A graph *H* is said to be a **subgraph** of graph *G* if and only if 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 an Undirected Graph

Let *G* be a undirected 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

Given a graph *G*=(*V*, *E*), the total degree of *G* = 2|E|.

The total degree of *G*
= deg(v_1) + deg(v_2) + … + deg(v_n)
= 2 × (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.

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 **$\deg^{-}$(*v*)**, is the number of directed edges that end at *v*. The **outdegree** of *v*, denoted **$\deg^{+}$(*v*)**, is the number of directed edges that originate from *v*.

Note that it only applies to directed
$\sum_{v \in V} deg^{-}(v) = \sum_{v \in V} deg^{+}(v) = |E|$

Definition: Connectedness

Two vertices *v* and *w* of a graph *G*=(*V*,*E*) are **connected** if and only if there is a walk from *v* to *w*.
The graph *G* is connected if and only if given *any* two vertices *v* and *w* in *G*, there is a walk from *v* to *w*. Symbolically,

G is connected iff ∀ vertices *v*, *w* ∈*V*, ∃ a walk from *v* to *w*.

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* ∈ {1, 2, …, *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.

A **path from *v* to *w*** is a trail that does not contain a repeated vertex.

A **closed walk** is a walk that starts and ends at the same vertex.

A **circuit** (or **cycle**) is a closed walk of length at least 3 that does not contain a repeated edge.

A **simple circuit** (or **simple cycle**) is a circuit that does not have any other repeated vertex except the first and last.

An undirected graph is **cyclic** if it contains a loop or a cycle; otherwise, it is **acyclic**.

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* if and only if

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*.

Definitions: Euler Circuit, Eulerian Graph

Let *G* be a graph. An **Euler circuit** for *G* is a circuit that contains every vertex and every edge of *G*.

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 does not 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 if and only if *G* is connected and every vertex of *G* has positive even degree.

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.

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* if and only if *G* is connected, *v* and *w* have odd degree, and all other vertices of *G* have positive even degree.

Definition: Hamiltonian Circuit

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.)

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.

Proposition 10.2.6 (Contrapositive)

If a graph *G* does *not* have a subgraph *H* with properties (1)–(4), then *G* does *not* have a Hamiltonian circuit.

Definition: Adjacency Matrix of a Directed Graph

Let *G* be a directed graph with ordered vertices $v_1, v_2, \dots v_n$. The **adjacency matrix of *G*** is the *n* × *n* matrix **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, …, *n*.

Definition: Adjacency Matrix of an Undirected Graph

Let *G* be an undirected graph with ordered vertices $v_1, v_2, \dots v_n$. The **adjacency matrix of *G*** is the *n* × *n* matrix **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, …, *n*.

Definition: n^{th} Power of a Matrix

For any *n* × *n* matrix **A**, the **powers of A** are defined as follows:

$\mathbf{A}^0 = \mathbf{I}$ where **I** is the *n* × *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 $v_1, v_2, \dots, v_m$ and **A** is the adjacency matrix of *G*, then for each positive integer *n* and for all integers *i*, *j* = 1, 2, …, *m*,

the *ij*-th entry of $\mathbf{A}^n$ = the number of walks of length *n* from v_i to v_j.

Definition: Isomorphic Graph

Let $G = (V_G, E_G)$ and $G' = (V_{G'}, E_{G'})$ be two graphs.

***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 ≅ be the relation of graph isomorphism on *S*. Then ≅ is an equivalence relation on *S*.

Definition: Planar Graph

A **planar graph** is a graph that can be drawn on a (two-dimensional) plane without edges crossing.

Kuratowski's Theorem:

A finite graph is planar if and only if it does not contain a subgraph that is a subdivision of the complete graph K_5 or the complete bipartite graph $K_{3,3}$.

Euler's Formula

$f = e - v + 2$

Hamiltonian graphs travel every vertex once (except first and last)
Eulerian graphs travel every edge once (except first and last)

Every complete graph has a Hamiltonian circuit

Tree

A **graph** is said to be **circuit-free** if and only if it has no circuits.

A graph is called a **tree** if and only 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** if and only if it is circuit-free and not connected.

Lemma 10.5.1

Any non-trivial tree has at least one vertex of degree 1.

Slide 12

All non-trivial trees actually have 2 vertices of degree 1

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**.

Theorem 10.5.2

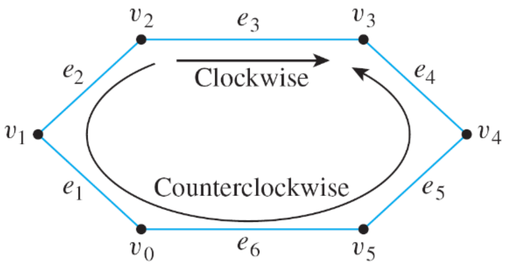
Any tree with *n* vertices (*n* > 0) has *n* – 1 edges.

Theorem 10.1.1 The Handshake Theorem

Given a graph *G*=(*V, E*), the total degree of *G* = 2|E|.

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.

Theorem 10.6.1: Full Binary Tree Theorem

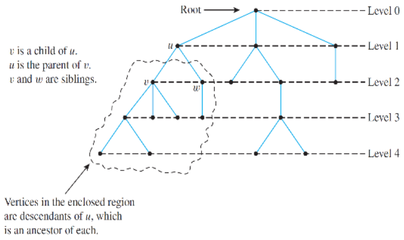
If *T* is a full binary tree with *k* internal vertices, then *T* has a total of 2*k* + 1 vertices and has *k* + 1 terminal vertices (leaves).

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.
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*.


Root
Level 0
Level 1
Level 2
Level 3
Level 4
u
v
w
v is a child of u.
u is the parent of v.
v and w are siblings.
Vertices in the enclosed region are descendants of u, which is an ancestor of each.

Theorem 10.6.2

For non-negative integers *h*, if *T* is any binary tree with height *h* and *t* terminal vertices (leaves), then $t \le 2^h$

Equivalently, $\log_2 t \le h$

Definitions: Binary Tree, Full Binary Tree

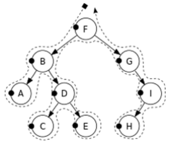
A **binary tree** is a rooted tree in which every parent has at most two children. Each child is designated either a **left child** or a **right child** (but not both), and every parent has at most one left child and one right child.

A **full binary tree** is a binary tree in which each parent has exactly two children.

Definitions: Left Subtree, Right Subtree

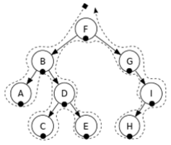
Given any parent *v* in a binary tree *T*, if *v* has a left child, then the **left subtree** of *v* is the binary tree whose root is the left child of *v*, whose vertices consist of the left child of *v* and all its descendants, and whose edges consist of all those edges of *T* that connect the vertices of the left subtree.

The **right subtree** of *v* is defined analogously.



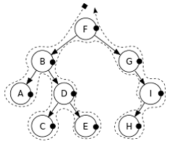
Pre-order:

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

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

Every connected graph has a spanning tree.

1. Any two spanning trees for a graph have the same number of edges
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 ***w*(*e*)** denotes the weight of *e* and ***w*(*G*)** denotes the total weight of *G*.

Kruskal's Algorithm:
Take the lowest weight edge, then add to the graph if it does not form a circuit

Prim's Algorithm
Start somewhere. Add the lowest weight among all the connected vertices.

Tutorial 10

A relation $\prec$ on a set A is said to be irreflexive, if and only if, $\forall a \in A, (a \nprec a)$.

Alternative definition of anti-symmetry: $\forall x, y\ (x \neq y) \Rightarrow ((x, y) \in R) \Rightarrow ((y, x) \notin R)$.

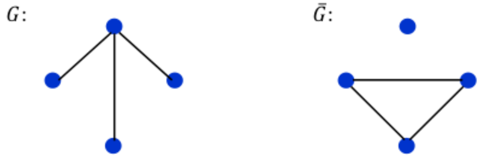
A relation is a strict partial order if and only if it is irreflexive, antisymmetric and transitive.

Let $\prec$ be a strict partial order on a set A. A subset C of A is called a chain if and only if each pair of distinct elements in C is comparable, that is, $\forall a, b \in C\ (a \neq b) \Rightarrow (a \prec b\ \lor\ b \prec a)$.

A maximal chain is a chain M such that $t \notin M \Rightarrow M \cup \{t\}$ is not a chain.

Tutorial 11

Definition 1. If G is a simple graph, the complement of G, denoted $\bar{G}$, is obtained as follows: the vertex set of $\bar{G}$ is identical to the vertex set of G. However, two distinct vertices v and w of $\bar{G}$ are connected by an edge if and only if v and w are not connected by an edge in G.



A graph G and its complement $\bar{G}$.

Definition 2. A self-complementary graph is isomorphic with its complement.

Definition 3. A simple circuit (cycle) of length three is called a triangle.

Lemma 10.5.5. Let G be a simple, undirected graph. Then if there are two distinct paths from a vertex v to a different vertex w, then G contains a cycle (and hence G is cyclic).

Q1b: Self-complementary graphs only exist for even number of edges.

Max possible edges of a graph is nC2

Q2: If G is a simple graph with n vertices where every vertex has degree at least $\lfloor n/2 \rfloor$. G is connected.

Q5: G is a simple undirected graph. If G is connected, $|E| \geqslant |V| - 1$ (Converse is false when unconnected)

Q6: if G is acyclic, $|E| \leqslant |V| - 1$ (converse is false where unconnected)

Unproven results:

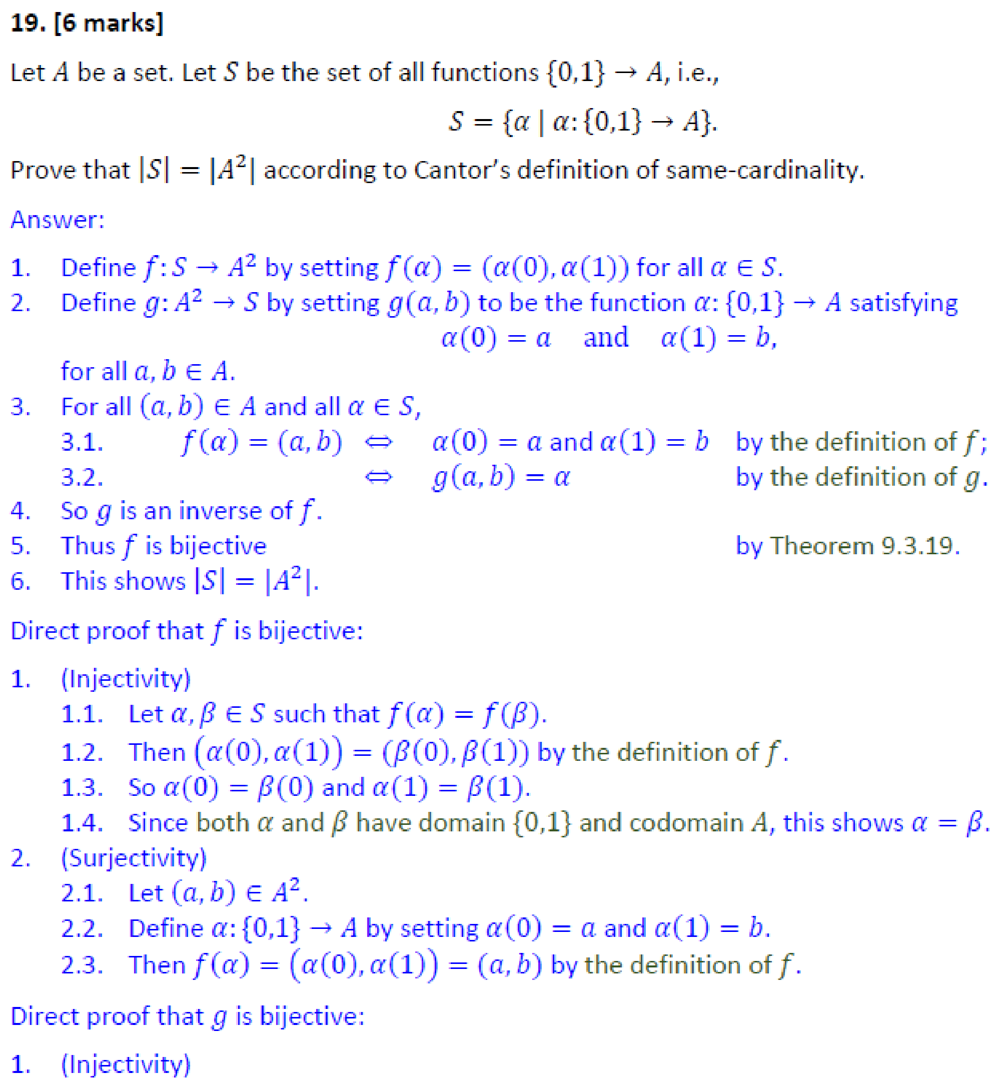
A tree with n nodes has n-1 edges.

There is a unique path between any two nodes of a tree.

Adding an edge between any two nodes of a tree creates a cycle

A graph is bipartite if, and only if, it does not contain any odd-length cycles.

Reflexive $\forall x \in A\ (xRx)$ All elements loop back Note that if A is empty, it is reflexive	Not reflexive $\exists x \in A\ (x\ !\ R\ x)$ At least 1 element does not loop back (Note that if A is no empty and R is empty, R is not reflexive because there is at least one element which does not loop back)
Symmetry $\forall x, y \in A\ (xRy \Rightarrow yRx)$ All two-headed arrow	Not symmetry $\exists x, y \in A\ (xRy \wedge y\ !\ R\ x)$ At least 1 non-two-headed arrow
Transitivity: $\forall x, y, z \in A\ (xRy \wedge yRz \Rightarrow xRz)$. If $a \to b$ and b → c, $a \to c$	Not transitive $\exists x, y, z \in A\ (x\ R\ y \wedge y\ R\ z \wedge x!\ Rz)$. At least 1 element where a ↛ c
Antisymmetric: $\forall x, y \in A\ (x\ R\ y \wedge y\ R\ x \Rightarrow x = y)$. If xRy and yRx, x=y. (Reflexivity is possible but not a req nor a guarantee) Used in partial orders, where there is some direction to it	Not antisymmetric $\exists x, y \in A\ (x\ R\ y \wedge y\ R\ x \wedge x \neq y)$. At least 1 double headed arrow with element not being itself
Irreflexive: $\forall x \in A\ (x\ (!\ R)\ x)$. There are no loops	Not irreflexive $\exists x \in A\ (xRx)$ At least one loop
Asymmetry: $\forall x, y \in A\ (x\ R\ y \Rightarrow\ y\ (!\ R)\ x)$. If xRy, y is not R (Must be irreflexive, there are no loops)	Not asymmetry $\exists x, y \in A\ (x\ R\ y \wedge\ y\ R\ x)$ At least one where x R y and y Rx



19. [6 marks]

Let A be a set. Let S be the set of all functions $\{0,1\} \to A$, i.e.,

$$S = \{\alpha \mid \alpha: \{0,1\} \to A\}.$$

Prove that $|S| = |A^2|$ according to Cantor's definition of same-cardinality.

Answer:

1. Define $f: S \to A^2$ by setting $f(\alpha) = (\alpha(0), \alpha(1))$ for all $\alpha \in S$.
2. Define $g: A^2 \to S$ by setting $g(a, b)$ to be the function $\alpha: \{0,1\} \to A$ satisfying
$$\alpha(0) = a \quad \text{and} \quad \alpha(1) = b,$$
for all $a, b \in A$.
3. For all $(a, b) \in A$ and all $\alpha \in S$,
   3.1. $f(\alpha) = (a, b) \iff \alpha(0) = a$ and $\alpha(1) = b$ by the definition of f;
   3.2. $\iff g(a, b) = \alpha$ by the definition of g.
4. So g is an inverse of f.
5. Thus f is bijective by Theorem 9.3.19.
6. This shows $|S| = |A^2|$.

Direct proof that f is bijective:

1. (Injectivity)
   1.1. Let $\alpha, \beta \in S$ such that $f(\alpha) = f(\beta)$.
   1.2. Then $(\alpha(0), \alpha(1)) = (\beta(0), \beta(1))$ by the definition of f.
   1.3. So $\alpha(0) = \beta(0)$ and $\alpha(1) = \beta(1)$.
   1.4. Since both α and β have domain $\{0,1\}$ and codomain A, this shows $\alpha = \beta$.
2. (Surjectivity)
   2.1. Let $(a, b) \in A^2$.
   2.2. Define $\alpha: \{0,1\} \to A$ by setting $\alpha(0) = a$ and $\alpha(1) = b$.
   2.3. Then $f(\alpha) = (\alpha(0), \alpha(1)) = (a, b)$ by the definition of f.

Direct proof that g is bijective:

1. (Injectivity)