Logic

Basic Notations
$\mathbb{R}$ set of real numbers
$\mathbb{Z}$ set of integers (includes 0)
$\mathbb{Q}$ set of rational numbers
$\mathbb{N}$ set of natural numbers (includes 0)
$\exists$ there exists...
$\exists!$ there exists a unique...
$\forall$ for all...
$\in$ member of...
s.t. such that...
$\rightarrow$ if...then…
$\leftrightarrow$ if, and only if/iff
Note: 0 is neither positive nor negative

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

Definition 2.1.6 (Logical Equivalence)
Two statement forms are called logically equivalent if, and only if, they have identical truth values for each possible substitution of statements for their statement variables. The logical equivalence of statement forms P and Q is denoted by P $\equiv$ Q.

Exclusive-Or
Denoted as p XOR q or p $\oplus$ q. Statement will only be true if only one of the variable is true
$$(p \vee q) \wedge \sim(p \wedge q)$$

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.

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.

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 $\rightarrow$ 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).

A conditional statement that is true because its hypothesis is false is called *vacuously true* or *true by default.*

Definition 2.2.2 (Contrapositive)
The contrapositive of p $\rightarrow$ q is ~q $\rightarrow$ ~p.

Definition 2.2.3 (Converse)
The converse of p $\rightarrow$ q is q $\rightarrow$ p.

Definition 2.2.4 (Inverse)
The inverse of p $\rightarrow$ q is ~p $\rightarrow$ ~q.

Equivalence
(Conditional) p $\rightarrow$ q $\equiv$ ~q $\rightarrow$ ~p (Contrapositive)
(Converse) p $\rightarrow$ q $\equiv$ ~p $\rightarrow$ ~q (Inverse)

Definition 2.2.5 (Only If)
If p and q are statements, "p only if q" means "if not q then not p" or "$\sim q \rightarrow \sim p$" Or, equivalently, "if p then q" or "$p \rightarrow q$"
Note: "p if q" means "if q then p" or "$q \rightarrow p$"

Definition 2.2.6 (Biconditional)
Given statement variables p and q, the biconditional of p and q is denoted p $\leftrightarrow$ q. It is true if both p and q have the same truth values and is false if p and q have opposite truth values

Definition 2.2.7 (Necessary & Sufficient Conditions)
If r and s are statements,
"r is a sufficient condition for s" means "if r then s" or "$r \rightarrow s$"

"r is a necessary condition for s" means "if not r then not s" or "if s then r" or "$s \rightarrow r$"

Order of Operations
First: ~ (also represented as ~).
No priority between $\wedge$ and $\vee$
p $\wedge$ q $\vee$ r is ambiguous
(p $\wedge$ q) $\vee$ r or p $\wedge$ (q $\vee$ r) is clear
Last: the implication, $\rightarrow$. Can be overwritten by parenthesis

Theorem 2.1.1 (Logical Equivalences)
Commutative Laws
$$p \wedge q \equiv q \wedge p$$
$$p \vee q \equiv q \vee p$$
Associative Laws
$$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$$
$$(p \vee q) \vee r \equiv p \vee (q \vee r)$$
Distributive Laws
$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$$
$$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$$
Identity Laws
$$p \wedge true \equiv p$$
$$p \vee false \equiv p$$
Negation Laws
$$p \vee \sim p \equiv true$$
$$p \wedge \sim p \equiv false$$
Double Negative Law
$$\sim(\sim p) \equiv p$$
Idempotent Laws
$$p \wedge p \equiv p$$
$$p \vee p \equiv p$$
Universal Bound Laws
$$p \vee true \equiv true$$
$$p \wedge false \equiv false$$
De Morgan's Laws
$$\sim(p \wedge q) \equiv \sim p \vee \sim q$$
$$\sim(p \vee q) \equiv \sim p \wedge \sim q$$
Absorption Laws
$$p \vee (p \wedge q) \equiv p$$
$$p \wedge (p \vee q) \equiv p$$
Negations of true and false
$$\sim true \equiv false$$
$$\sim false \equiv true$$

Implication Law (Not under Theorem 2.1.1)
$$p \rightarrow q \equiv \sim p \vee q$$
$$\sim(p \rightarrow q) \equiv p \wedge \sim q$$

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 $\cdot$ / $\therefore$, 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.

Rules of Inference
Modus ponens
$$p \rightarrow q$$
$$p$$
$$\cdot\ q$$
Modus tollens
$$p \rightarrow q$$
$$\sim q$$
$$\cdot \sim p$$
Generalization
$$P$$
$$\cdot\ p \vee q$$
Specialization
$$p \wedge q$$
$$\cdot\ p$$
Elimination
$$p \vee q$$
$$\sim q$$
$$\cdot\ p$$
Transitivity
$$p \rightarrow q$$
$$q \rightarrow r$$
$$\cdot\ p \rightarrow r$$
Proof by Division into Cases
$$p \vee q$$
$$p \rightarrow r$$
$$q \rightarrow r$$
$$\cdot\ r$$
Contradiction Rule
$$\sim p \rightarrow false$$
$$\cdot\ p$$

Fallacies
Converse Error
$$p \rightarrow q$$
$$q$$
$$\cdot\ p$$
Inverse Error
$$p \rightarrow q$$
$$\sim p$$
$$\cdot \sim q$$
False premise
- Valid but unsound argument as premise is false

Definition 3.1.1 (Predicate)
A predicate is a sentence that contains a finite number of variables and becomes a statement when specific values are substituted for the variables. The domain of a predicate variable is the set of all values that may be substituted in place of the variable.

Definition 3.1.2 (Truth set)
If P(x) is a predicate and x has domain D, the truth set is the set of all elements of D that make P(x) true when they are substituted for x. The truth set of P(x) is denoted {x ∈ D | P(x)}.

Definition 3.1.3 (Universal Statement)
Let Q(x) be a predicate and D the domain of x. A universal statement is a statement of the form

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

It is defined to be true iff Q(x) is true for every x in D. It is defined to be false iff Q(x) is false for at least one x in D.
A value for x for which Q(x) is false is called a counterexample.

Definition 3.1.4 (Existential Statement)
Let Q(x) be a predicate and D the domain of x. An existential statement is a statement of the form

$$\exists x \in D \; s.t. \; Q(x)$$

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

Theorem 3.2.1 (Negation of Universal State.)
The negation of a statement of the form

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

is logically equivalent to a statement of the form

$$\exists x \in D \; s.t. \sim P(x)$$

Theorem 3.2.2 (Negation of Existential State.)
The negation of a statement of the form

$$\exists x \in D \; s.t. \; P\,(x)$$

is logically equivalent to a statement of the form

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

Definition 3.2.1 (Contrapositive, converse, inverse of Universal Conditonal State.)
Same as conditional statements

Definition 3.2.2 (Necessary and Sufficient conditions, Only if of Universal Conditional State.)
Same as Conditional Statements

Vacuously True
Can be applied to conditional statements, universal conditional statements and universal statements
- statements are vacuously true iff hypothesis is false/predicate, P(x) is false for every x ∈ D (or D is empty)

Universal & Existential General Rule
'All boys wear glasses' is written as

$$\forall x(Boy(x) \rightarrow Glasses(x))$$

If conjunction was used, this statement would be falsified by the existence of a 'non-boy' in the domain of x.

'There is a boy who wears glasses' is written as

$$\exists x(Boy(x) \wedge Glasses(x))$$

If implication was used, this statement would true even if the domain of x is empty.

Multiply-Quantified Statements
To establish the truth of statements:

$$\forall x \in D, \exists y \in E \; s.t. P(x, y)$$

Given any x in D, find a y in E that works for that particular x

$$\exists x \in D \; s.t. \forall y \in E, P(x, y)$$

Find a particular x in D that will work for any y in E

Negation of Multiply-Quantified Statements

$$\sim \big(\forall x \in D, \exists y \in E \; s.t. P(x, y)\big)$$
$$\equiv$$
$$\exists x \in D \; s.t. \forall y \in E, \sim P(x, y)$$

Order of Quantifiers
Order matters if quantifiers are different e.g., both ∀ and ∃. Order doesn't matter if all quantifiers are the same

Implicit Quantification
The notation $P(x) \rightarrow Q(x)$ means that every element in the truth set of P(x) is in the truth set of Q(x), or equivalently, $\forall x, P(x) \rightarrow Q(x)$.
The notation $P(x) \leftrightarrow Q(x)$ means that P (x) and Q(x) have identical truth sets, or equivalently, $\forall x, P\,(x) \leftrightarrow Q(x)$

Universal Instantiation
If some property is true of everything in a set, then it is true of any particular thing in the set.

Rules of Inference for Quantified Statements
Universal Modus ponens

$$\forall x \in D, (P(x) \rightarrow Q(x))$$
$$P(a) \; for \; particular \; a \in D$$
$$\cdot \; Q(a)$$

Universal Modus tollens

$$\forall x \in D, (P(x) \rightarrow Q(x))$$
$$\sim Q(a) \; for \; particular \; a \in D$$
$$\cdot \sim P(a)$$

Universal Transitivity

$$\forall x \; (P(x) \rightarrow Q(x))$$
$$\forall x \; (Q(x) \rightarrow R(x))$$
$$\cdot \; \forall x \; (P(x) \rightarrow R(x))$$

Universal Instantiation

$$\forall x \in D, P(x)$$
$$\cdot \; P(a) \; if \; a \in D$$

Universal Generalisation

$$P(a) \; for \; every \; a \in D$$
$$\cdot \; \forall x \in D, P(x)$$

Existential Instantiation

$$\exists x \in D, P(x)$$
$$\cdot \; P(a) \; if \; a \in D$$

Existential Generalisation

$$P(a) \; for \; some \; a \in D$$
$$\cdot \; \exists x \in D, P(x)$$

Definition 3.4.1 (Valid Argument Form)
To say that an argument form is valid means the following: No matter what particular predicates are substituted for the predicate symbols in its premises, if the resulting premise statements are all true, then the conclusion is also true. An argument is called valid if, and only if, its form is valid.

Valid Arguments as Tautologies
All valid arguments can be restated as tautologies.

Additional Notes (Valid Argument as Tautology)
Given an argument:

$$p1$$
$$p2$$
$$\vdots$$
$$pk$$
$$\therefore q$$

where $p1, p2, \ldots, pk$ are the k premises and q the conclusion, we can say that "the argument is valid if and only if $(p1 \wedge p2 \wedge \cdots \wedge pk) \longrightarrow q$ is a tautology"

Proving Valid Arguments
- by truth table, where all critical rows' (row where all premises are true) conclusion is true
- by proving the argument is a tautology
  - rearrange into a conditional statement
- proof by contradiction
  1. premises arise to contradiction, hence argument vacuously valid
  2. assume argument is invalid (take conclusion as false), if contradiction arise, argument is valid

You can utilize rules of inference, conjunction of premises to arrive at conclusion
- as you are assuming all premises to be true to check if conclusion is also true

Set Theory

Set
- unordered collection of elements
- order and duplicates do not matter

Set-Roster Notation
A set may be specified by writing all of its elements between braces e.g., {2,3,4}, {1,2,3,…}

Set-Builder Notation (members that fulfil predicate)
Let U be a set and $P(x)$ be a **predicate** over U. Then the set of all elements $x \in U$ such that $P(x)$ is true is denoted

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

Replacement Notation (apply term on members)
Let A be a set and $t(x)$ be a **term** in a variable x. Then the set of all objects of the form $t(x)$ where x ranges over the elements of A is denoted

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

Definition: Membership of a Set (Notation: ∈)
If S is a set, the notation $x \in S$ means that x is an element of S. ($x \notin S$ means x is not an element of S.)

Definition: Cardinality of a Set (Notation: $|S|$)
The cardinality of a set S, denoted as $|S|$, is the size of the set, that is, the number of elements in S.

Definition: Subsets & Superset
A is a subset of B, written $A \subseteq B$, iff every element of A is also an element of B. Symbolically,

$$A \subseteq B \Leftrightarrow \forall x(x \in A \rightarrow x \in B)$$

Definition: Proper Subset
Let A and B be sets. A is a proper subset of B, denoted $A \subsetneq B$, iff $A \subseteq B$ and $A \neq B$. In this case, we may say that the inclusion of A in B is proper or strict

Definition: Empty Set
An empty set has no element and is denoted $\emptyset$

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

$$A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A.$$

Or from definition of subsets:

$$A = B \Leftrightarrow \forall x\,(x \in A \Leftrightarrow x \in B)$$

Proving Set Equality (A=B)
- Prove A is a subset of B $(x \in A \Rightarrow x \in B)$
- Prove B is a subset of A $(x \in B \Rightarrow x \in A)$

Definition: Union (in A or B)

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

Definition: Intersection (in A and B)

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

Definition: Set difference (in B not in A)

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

Definition Set complement (not in A)

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

Definition (Power Sets)
Given a set A, the power set of A, denoted $\mathcal{P}(A)$, is the set of all subsets of A
For example,

$$let\ A = \{x, y\}$$
$$\mathcal{P}(A) = \{\phi, \{x\}, \{y\}, \{x, y\}\}$$

Definition: Disjoint (no elements in common)
A and B are disjoint iff $A \cap B = \emptyset$

Definition: 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,

$$\forall i, j \in \{1,2,3,\ldots\},\ i \neq j \rightarrow A_i \cap A_j = \emptyset$$

Unions and Intersections of an Indexed Collection of Sets
Given sets A_0, A_1, A_2 … that are subsets of a universal set U and a given nonnegative integer n,

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

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

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

$$\bigcap_{i=0}^{\infty} A_i = \{x \in U \mid x \in A_i \text{ for all non} -\text{ve integer } i\}$$

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:

$$(a, b) = (c, d) \Leftrightarrow (a = c) \wedge (b = d)$$

Definition: Ordered n-tuples
Let $n \in \mathbb{Z}^+$ and let $x_1, x_2, \cdots, x_n$ be (not necessarily distinct) elements. An ordered $\boldsymbol{n}$-tuple is an expression of the form $(x_1, x_2, \cdots, x_n)$

$$(x_1, x_2, \cdots, x_n) = (y_1, y_2, \cdots, y_n)$$
$$\Leftrightarrow x_1 = y_1, x_2 = y_2, \cdots, xn = yn$$

Definition: Cartesian Product
Given sets A and B, the Cartesian product of A and B, denoted $\boldsymbol{A} \times \boldsymbol{B}$, is the set of all ordered pairs (a, b) where a is in A and b is in B. Symbolically:

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

For example,

$$\{1, 2, 3\} \times \{a, b\} =$$
$$\{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$$

Definition: Generalised Cartesian Product
Given sets $A_1, A_2, \cdots, A_n$,

$$A_1 \times A_2 \times \cdots \times A_n =$$
$$\{a_1, a_2, \cdots, a_n : a_1 \in A_1 \wedge a_2 \in A_2 \wedge \cdots \wedge a_n \in A_n\}$$

If A is a set, then $A^n = A \times A \times \cdots \times A$ (n times)

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. $(a, b) \in X \times Y \Leftrightarrow a \in X \wedge b \in Y$

Note: In a context where U is the universal set (so that implicitly means $U \supseteq X$), the complement of X, denoted $\bar{X}$,is defined by $\bar{X} = U \setminus X$.

Theorem 6.2.4 (Empty set subset of all sets)
An empty set is a subset of all sets.

$$\forall A, A\ is\ a\ set, \emptyset \subseteq A$$

Theorem (Cardinality of Power Set of a Finite Set)
Let A be a finite set where $|A| = n$, then $|\mathcal{P}(A)| = 2^n$

Theorem 6.3.1
Suppose A is a finite set with n elements, then $\mathcal{P}(A)$ has 2^n elements. In other words, $\mathcal{P}\ A = 2^{|A|}$.

Theorem 6.2.1 (Some subset relations)
Inclusion of Intersection

$$A \cap B \subseteq A$$
$$A \cap B \subseteq B$$

Inclusion in Union

$$A \subseteq A \cup B$$
$$B \subseteq A \cup B$$

Transitive Property of Subsets

$$A \subseteq B \wedge B \subseteq C \rightarrow A \subseteq C$$

Theorem 6.2.2 (Set Identities)
Let all sets referred to below be subsets of a universal set U. ~ is used in replacement of set complement

Commutative Laws

$$A \cup B = B \cup A$$
$$A \cap B = B \cap A$$

Associative Laws

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

Distributive Laws

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

Identity Laws

$$A \cup \emptyset = A$$
$$A \cap U = A$$

Complement Laws

$$A \cup \bar{A} = U$$
$$A \cap \bar{A} = \emptyset$$

Double Complement Law

$$\bar{\bar{A}} = A$$

Idempotent Laws

$$A \cup A = A$$
$$A \cap A = A$$

Universal Bound Laws

$$A \cup U = U$$
$$A \cap \emptyset = \emptyset$$

De Morgan's Laws

$$\overline{(A \cup B)} = \bar{A} \cap \bar{B}$$
$$\overline{(A \cap B)} = \bar{A} \cup \bar{B}$$

Absorption Laws

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

Complements of U and $\emptyset$

$$\bar{U} = \emptyset$$
$$\bar{\emptyset} = U$$

Set Difference Law

$$A \setminus B = A \cap \bar{B}$$

Proving Subsets (A ⊆ B)
- let x ∈ A
- then show x ∈ B

Relations

Definition: Relation
Let A and B be sets. A (binary) relation from $\boldsymbol{A}$ to $\boldsymbol{B}$ is a subset of $\boldsymbol{A} \times \boldsymbol{B}$.

$$x\ R\ y \text{ means } (x, y) \in R$$
$$x\ \not{R}\ y \text{ means } (x, y) \notin R$$

Definitions: Domain, Co-domain, Range
Let A and B be sets and R be a relation from A to B.
The domain of R,

$$Dom(R) = \{a \in A : aRb \text{ for some } b \in B\}$$

The co-domain of R,

$$coDom(R) = B.$$

The range of R,

$$Range(R) = \{b \in B: aRb \text{ for some } a \in A\}$$

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

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

or

$$\forall x \in A, \forall y \in B\ (\ (y, x) \in R^{-1} \Leftrightarrow (x, y) \in R)$$
$$\text{Also, } \forall x \in A, \forall y \in B\ (yR^{-1}x \Leftrightarrow xRy)$$

Definition: Relation on a Set
A relation on a set $\boldsymbol{A}$ is a relation from A to A. In other words, a relation on a set A is a subset of $A \times A$

Definition: $\boldsymbol{n}$-ary Relation
Given n sets $A_1, A_2, \cdots, A_n$, an $\boldsymbol{n}$-ary relation $\boldsymbol{R}$ on $A_1 \times A_2 \times \cdots \times A_n$ is a subset of $A_1 \times A_2 \times \cdots \times A_n$

Definition: Composition of Relations
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:

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

Proposition: Composition is Associative
Let A, B, C, D be sets. Let $R \subseteq A \times B$, $S \subseteq B \times C$ and $T \subseteq C \times D$ be relations.

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

Proposition: Inverse of Composition
Let A, B and C be sets. Let $R \subseteq A \times B$ and $S \subseteq B \times C$ be relations.

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

Definitions: Reflexivity
R is reflexive iff $\forall x \in A\ (xRx)$

Definition: Symmetry
R is symmetric iff $\forall x, y \in A\ (xRy \Rightarrow yRx)$

Definition: Transitivity
R is transitive iff $\forall x, y, z \in A\ (xRy \wedge yRz \Rightarrow xRz)$

Definition: Antisymmetry
Let R be a relation on a set A. R is antisymmetric iff

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

Note: antisymmetry ≢ non-symmetry

Definition: Asymmetry (Tutorial 5)
R is asymmetric iff $\forall x, y \in A\ (x\ R\ y \Rightarrow y\ \not{R}\ x)$

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

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

Intuitively, can be understood as the relation obtained by adding the least number of ordered pairs to ensure transitivity

Reflexive Closure (Tutorial 5 Q5)
The reflexive closure S of a relation R on a set A is obtained by adding (a, a) to R for each a ∈ A.
Symbolically, $S = R \cup \{(x, x) : x \in X\}$.

Definition: Partition
C is a partition of a set A if the following hold:
(1) C is a set of which all elements are non-empty subsets of A,

$$\emptyset \neq S \subseteq A \text{ for all } S \in C$$

(2) Every element of A is in exactly one element of C,

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

Or simply,

$$\forall x \in A\ \exists!\ S \in C\ (x \in S)$$

Elements of a partition are called components

In layman's, a partition of a set A is a finite or infinite set of nonempty, mutually disjoint subsets whose union is A (every element of A is in exactly one component of C)

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. $x, y \in S$
*x is in same component, S as y

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

Definition: Equivalence Class
Suppose A is a set and ~ is an equivalence relation on A. For each $a \in A$, the equivalence class of a, denoted $[\boldsymbol{a}]$ is the set of all elements $x \in A$ s.t. a is ~-related to x. Symbolically,

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

Definition: Set of equivalence classes (≡ partition)
Let A be a set and ~ be an equivalence relation on A. Denote by $A/\sim$ the set of all equivalence classes with respect to ~,

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

Definition: Congruence
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 $k \in \mathbb{Z}$. Symbolically

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

Proposition (Lecture 6 Slide 54)
Congruence-mod n is an equivalence relation on $\mathbb{Z}$ for every $n \in \mathbb{Z}^+$.

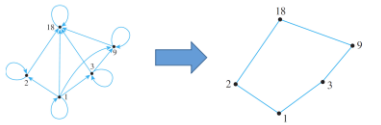
Definition: Partial Order Relation
Let R be a relation on a set A. Then R is a partial order relation (or simply partial order) denoted using $\preccurlyeq$ iff R is reflexive, antisymmetric and transitive

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: 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.

Hasse Diagrams
The Hasse diagram is a simplified directed graph.

1. Draw the directed graph so that all arrows point upwards.
2. Eliminate all self-loops.
3. Eliminate all arrows implied by transitivity.
4. Remove the direction of the arrows.



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

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

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

Definition: Compatible
Elements a, b are compatible iff there exists c ∈ A such that a ⪯ c and b ⪯ c.

Definition: Maximal
Let $\preccurlyeq$ be a partial order on the set A and $c \in A$. c is a maximal element of A iff

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

Definition: Largest/Maximum
Let $\preccurlyeq$ be a partial order on the set A and $c \in A$. c is the largest element of A iff

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

Definition: Minimal
Let $\preccurlyeq$ be a partial order on the set A and $c \in A$. c is a minimal element of A iff

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

Definition: Smallest/Minimum
Let $\preccurlyeq$ be a partial order on the set A and $c \in A$. c is the largest element of A iff

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

Proposition: A smallest element is minimal (Lec 6)
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

$$R \text{ is a partial order and } \forall x, y \in A\ x\ R\ y \vee y\ R\ x$$

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

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

(View set A as a set of tasks. $x \preccurlyeq y$ means x must be performed before y. If $x \not\preccurlyeq y$, then x and y can be performed in any order w.r.t each other)

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,

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

not just R; but A also

Kahn's Algorithm

Input: A finite set A and a partial order $\preccurlyeq$ on A.

1. Set $A_0 := A$ and $i := 0$.
2. Repeat until $A_i = \emptyset$
   2.1 find a minimal element c_i of A+ wrt $\preccurlyeq$
   2.2. set $A_i + 1 = A_i \setminus \{c_i\}$
   2.3. set $i := i + 1$

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

$$c_i \preccurlyeq^* c_j \Leftrightarrow i \leq j$$

Theorem 8.3.1 (Equivalence Relation by 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

Theorem 8.3.4 (Partition by Equivalence Relation)
If A is a set and R is an equivalence relation on A, then the set of distinct equivalence classes of R form a partition of A

Lemma Rel.1 (Equivalence Classes)
Let ~ 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) $[x] \cap [y] \neq \emptyset$

Theorem Rel.2 (Equivalence classes form partition)
Let ~ be an equivalence relation on a set A. Then $A/\sim$ is a partition of A

Congruence mod n distinct equivalence classes

$$\{nk : k \in \mathbb{Z}\}$$
$$\{nk + 1 : k \in \mathbb{Z}\}$$
...
$$\{nk + (n-1) : k \in \mathbb{Z}\}$$

Proof of Reflexivity
- suppose x ∈ Set
- utilise given relation definition to show xRx
- hence R is reflexive

Proof of Symmetry
- suppose x,y ∈ Set, s.t. xRy
- utilise given definition of relation
- show inverse also fulfils given definition
- hence yRx and R is symmetric

Proof of Transitivity
- suppose x,y,z ∈ Set, s.t. xRy and yRz
- utilise given definition of relation
- show x and z also fulfils definition
- hence xRz and R is transitive

Proof of Anti-symmetry
- suppose x,y ∈ Set, s.t. xRy and yRx
- utilise given definition of relation
- show x = y
- hence R is anti-symmetric

Proof of Partitions ($A/\sim$ is a partition of A)
- $A/\sim$ is by definition a set
- show that every element of $A/\sim$ is a nonempty subset of A
(show element is a subset of A, then show element minimally contains one member due to reflexivity)
- show every element of A is in at least one element of $A/\sim$
(utilize reflexivity)
- show every element of A is in at most one element of $A/\sim$
(assume element of A is in two elements, S_1, S_2 of $A/\sim$, then show $S_1 = S_2$)

1. ☑ In a partially ordered set, any smallest element is minimal.
2. ☑ All finite non-empty partially ordered sets have a minimal element.
3. ☑ In a partially ordered set, if there is a smallest element, there must be exactly one minimal element.
4. ☑ An infinite set partial order relation can have a smallest element. (example: consider the divisibility relation on $\mathbb{Z}^+$, 1 is the smallest element).
5. ✗ A relation that is symmetric cannot be antisymmetric. → empty relation
6. ✗ A relation that is not symmetric must be antisymmetric. → {(1,2),(3,4),(4,3)}
7. ✗ In a partially ordered set, any minimal element is smallest.
8. ✗ There can be 2 smallest elements in some partially ordered set.
9. ✗ In a partially ordered set, if there is exactly one minimal element, then there is a smallest element. (notice that the set can be infinite with a single lone element on the side of the linear hasse diagram, which would be the minimal, as well as maximal, element).
10. ✗ If a partially ordered set does not have a smallest element, it must be an infinite set.

Tutorial Proofs

Proof (Tutorial 4 Q2)
Let R be a relation on set A. The following are equivalent for all $x, y \in A$.

(i) symmetric, $x\,R\,y \Rightarrow y\,R\,x$
(ii) $x\,R\,y \Leftrightarrow y\,R\,x$
(iii) $R = R^{-1}$

Proof (Tutorial 4 Q9(a))
If x ∈ S ∈ C, then [x] = S. (If x is an element of a component S which is an element of a partition, then the equivalence class of x is S.)

Proof (Tutorial 4 Q9(b))
A/~ = C (The set of equivalence classes of A is a partition of A.)

Proof (Tutorial 5 Q3)
Binary relation ⊆ on P(A) is a partial order.

Proof (Tutorial 5 Q6(c))
For a relation R, if R is asymmetric then R is antisymmetric

antisymmetric & not reflexive

Proof (Tutorial 5 Q10(a))
In all partially ordered sets, if two elements are comparable then they are compatible.
(In all partially ordered sets, any two comparable elements are compatible)

T4Q5: for all equivalence rltns R;
$R = R^{-1}$; $R = R \circ R$
and all permutations; ⊆ of this apply

Functions

Definition: Function
A function f from a set X to a set Y, denoted f : X → Y, is a relation satisfying the following properties:
(F1) ∀x ∈ X ∃y ∈ Y (x, y) ∈ f
(every input has an output)
(F2) ∀x ∈ X ∀y_1, y_2 ∈ Y (((x, y_1) ∈ f ∧ (x, y_2) ∈ f) → y_1 = y_2)
(every input has only one output)

Definitions: Arg, image, pre-image, 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 $x \to_f y$ or $f: x \mapsto y$. 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.

Definition: Setwise image and preimage
Let f : X → Y be a function from set X to set Y and f : P(X) → P(Y)
• If A ⊆ X, then let f(A) = {f(x) : x ∈ A}.
• If B ⊆ Y , then let f^{-1}(B) = {x ∈ X : f(X) ∈ B}.
We call f(A) the **(setwise) image** of A, and f^{-1}(B) the **(setwise) preimage** of B under f

Definition: Domain, Co-domain and Range
Let $f: A \to B$ be a function from set A to set B.
▪ A is the **domain** of f and B the **co-domain** of f.
▪ The **range** of f is the (setwise) image of A under f: $\{b \in B : b = f(a)$ for some $a \in A\}$.

Definition: Sequence (of infinite length)
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 $n \in \mathbb{Z}_{\geq 0}$.

Definition: 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 (of finite length)
Let A be a set. A **string** or a word over A is an expression of the form $a_0a_1a_2 \cdots a_{l-1}$ 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.

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 $n \in \mathbb{Z}_{\geq 0}$

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 $i \in \{0,1,2, \ldots, l-1\}$

Theorem 7.1.1 (Function Equality)
Two functions $f: A \to B$ and $g: C \to D$ are equal, $f = g$, iff (i) $A = C$ and $B = D$, and (ii) $f(x) = g(x)$ $\forall x \in A$
both conditions!

Definition: Injection (one to one)
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

Definition: Surjection (onto)
A function $f: X \to Y$ is surjective (or onto) iff
$$\forall y \in Y\ \exists x \in X\ (y = f(x))$$
Every element in the co-domain has at least one preimage. So, range = co-domain. A surjective function is called a surjection

Definition: Bijection
A function $f: X \to Y$ is bijective iff f is injective and surjective, i.e.
$$\forall y \in Y\ \exists!\ x \in X\ (y = f(x))$$
A bijective function is called a bijection or one-to-one correspondence.

Definition: Inverse Functions
Let $f: X \to Y$. Then $g: Y \to X$ is an inverse of f iff
$$\forall x \in X\ \forall y \in Y\ (y = f(x) \Leftrightarrow x = g(y))$$
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:
$$(g \circ f)(x) = g(f(x))\ \forall x \in X.$$
where $g \circ f$ is read "g circle f" and $g\ f\ x$ is read "g of f of x". The function $g \circ f$ is called the **composition** of f and g.

Definition: Identity
$$id_X(x) = x \text{ for all } x \in X$$

Theorem 7.3.1 (Composition with 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
iff
$$f \circ id_X = f \text{ and } id_Y \circ f = f$$
diff!

Theorem 7.3.2 (Composition of Function w Inverse)
If $f: X \to Y$ is a bijection with inverse function $f^{-1}: Y \to X$, then
$$f^{-1} \circ f = id_X \text{ and } f \circ f^{-1} = id_Y$$

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.

Definition: Addition and Multiplication on $\mathbb{Z}_n$
$\mathbb{Z}_n$: congruence-mod-n relation on $\mathbb{Z}$
Define addition + and multiplication · on $\mathbb{Z}_n$ as follows: whenever $[x], [y] \in \mathbb{Z}_n$,
$$[x] + [y] = [x + y] \text{ and } [x] \cdot [y] = [x \cdot y]$$

Proposition: Addition on $\mathbb{Z}_n$ is well defined
For all $n \in \mathbb{Z}^+$ and all $[x1], [y1], [x2], [y2] \in \mathbb{Z}_n$,
$[x1] = [x2]$ and $[y1] = [y2] \Rightarrow [x1] + [y1] = [x2] + [y2]$

Proposition: Multiplication on $\mathbb{Z}_n$ is well defined
For all $n \in \mathbb{Z}^+$ and all $[x1], [y1], [x2], [y2] \in \mathbb{Z}_n$,
$[x1] = [x2]$ and $[y1] = [y2] \Rightarrow [x1] \cdot [y1] = [x2] \cdot [y2]$

Definition: Well-Defined Function property
∀x1, x2 ∈ X, ∀f : X → Y, x1 = x2 → f(x1) = f(x2)

Definition: Well-Defined property wrt Equiv Rel.
∀x1, x2 ∈ X, ∀f : X → Y, x1∼x2 → f(x1)∼f(x2)

Definition: Well-Defined property wrt Equiv Class
∀x1, x2 ∈ X, ∀f : X → Y, [x1] = [x2] → [f(x1)] = [f(x2)]

Tutorial Proofs

Proof (Tutorial 6 Q7)
If $f: B \to C$ and function g with domain C s.t. $g \circ f$ is injective, then f is injective

Proof (Tutorial 6 Q9)
Given $f: A \to B$. Let $X \subseteq A$ and $Y \subseteq B$.
Then $X \subseteq f^{-1}(f(X))$ and $f(f^{-1}(Y)) \subseteq Y$

Proof (Tutorial 6 Q6)
A function is injective iff it has a left inverse
A function is surjective iff it has a right inverse

Left/Right Inverse Definition
Given a function $f: A \to B$, we say that
$g: B \to A$ is a left inverse of f if and only if $g(f(a)) = a$ for all $a \in A$.
$h: B \to A$ is a right inverse of f if and only if $f(h(b)) = b$ for all $b \in B$.

Order of a bijection
The order of a bijection $f: A \to A$ is defined to be the smallest $n \in \mathbb{Z}^+$ such that
$$f \circ f \circ \cdots \circ f = idA.$$
n-many f's

Mathematical Induction

Theorem 5.1.1 (Props. of Summation and Products)
If a_m, a_{m+1}, a_{m+2}, ⋯ and b_m, b_{m+1}, b_{m+2}, ⋯ are sequences of real numbers and c is any real number , then the following equations hold for any integer $n \geq m$:

$$\sum_{k=m}^{n} a_k + \sum_{k=m}^{n} b_k = \sum_{k=m}^{n} (ak + bk)$$

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

$$(\prod_{k=m}^{n} a_k) \cdot (\prod_{k=m}^{n} b_k) = \prod_{k=m}^{n} (ak \cdot bk)$$

Definitions: 1P1 (First prin. Of MI)
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.

Definition: 2PI (Second prin. Of MI)
Let P(n) be a property that is defined for integers n, and let a and b be fixed integers with a b. Suppose the following 2 statements are true:
1. P(a), P(a + 1),...,P(b) are all true
2. For all integers $k \geq$ b, if P(i) is true for all integers i from a through k, then $P(k + 1)$ is true.

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

Theorem 5.2.2 (Sum of First n integers)
For all integers $n \geq 1$,

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

Theorem 5.2.3 (Sum of GP)
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
For all integers $n \geq 0$, $2^{2n} - 1$ is divisible by 3

Proposition 5.3.2
For all integers $n \geq 3$, $2n + 1 < 2^n$

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

Definition: Recurrence relation
A recurrence relation for a sequence a_0, a_1, a_2, ⋯ is a formula that relates each term a_k to certain of its predecessors a_{k-1}, a_{k-2}, ⋯ , 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, ⋯ , a_{i-1}.
If i depends on k, the initial conditions specify the values of a_0, a_1, a_2, ⋯ , a_m, where m is an integer with $m \geq 0$.

Definition: Recursive definition of 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:

1. (basis step) show that $P(c)$ is true for every founder c; and
2. (induction step) show that $\forall x \in S\ P\ x \Rightarrow P\ f\ x$ 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

Tutorial Proofs

Proof (Tutorial 7 Q2)
For all $n \in \mathbb{Z}+$,

$$1^2 + 2^2 + \cdots + n^2 = \frac{1}{6} n(n + 1)(2n + 1)$$

Proof (Tutorial 7 Q3)
Let $x \in \mathbb{R}_{\geq -1}$. For all $n \in \mathbb{Z}^+$,

$$1 + nx \leq (1 + x)n$$

Proof (Tutorial 7 Q5)
For all $n \in \mathbb{Z}^+$,

$$2^{n+2} \mid a^{2^n} - 2$$

$\forall n \in \mathbb{Z}_{\geq 8}$ $\exists x, y \in \mathbb{N}$ $n = 3x + 5y$.

Q6: Every positive integer can be written as sum of distinct non-negative integer powers of 2.

1PI Steps
1. Let P(n) ≡ …
2. Basis: Prove P(a)
3. Inductive hypothesis: Assume P(k) is true for $k \geq a$, that is …
4. Inductive Step: show P(k+1) is true

2PI Steps
1. Let P(n) ≡ …
2. Basis: Prove P(a), P(a+1) …
3. Inductive Hypothesis: Assume P(i) is true for a ≤ i ≤ k
4. Inductive Step: show P(k+1) is true

Cardinality

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

Definition: Finite set and Infinite set
Let $\mathbb{Z}_n = \{1,2,3, \dots, n\}$, 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
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 $f: A \to B$

Theorem 7.4.1 (Properties of Cardinality)
The same-cardinality relation is an **equivalence relation**. For all sets A, B and C:
a. Reflexive: $|A| = |A|$.
b. Symmetric: $|A| = |B| \to |B| = |A|$.
c. Transitive: $(|A| = |B|) \wedge (|B| = |C|) \to |A| = |C|$

Definition: Cardinal Numbers
Define $\aleph_0 = |\mathbb{Z}^+|$. (Some authors 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 $|S| = \aleph_0$

Definition: Countable 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

Theorem (Cartesian Product)
If sets A and B are both countably infinite, then so is $A \times B$

Corollary (General Cartesian Product)
Given $n \geq 2$ 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

$$\bigcup_{i=1}^{\infty} A_i$$

only up to $i = n$, $n \in \mathbb{Z}$

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
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 T 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.

Tutorial Proofs

Proof (Tutorial 8 Q2)
If A is countably infinite and B is finite, then A ∪ B is countable

Proof (Tutorial 8 Q3)
If $A_1, A_2, A_3, \cdots$ are finite sets, then $\bigcup_{i=1}^{n} A_i$ is finite for any $n \geq 2$

Proof (Tutorial 8 Q4)
If $A_1, A_2, A_3, \cdots$ are countable sets, then $\bigcup_{i=1}^{n} A_i$ is countable for any $n \in \mathbb{Z}^+$

Proof (Tutorial 8 Q5)
If S_i is countably infinite for each $i \in \mathbb{Z}^+$, then $\bigcup_{i \in \mathbb{Z}^+} S_i$ is countable. Countable union of countably infinite set is countable

Proof (Tutorial 8 Q6)
If B is infinite and C is finite, then there exists a bijection B ∪ C → B

Proof (Tutorial 8 Q7)
If A is countably infinite, then powerset, P(A) is uncountable.

$\mathbb{N}$ is countable

Counting

Definition: Sample Space and Event
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 (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 (Multiplication Rule)
If an operation consists of k steps and the first step can be performed in n_1 ways, the second step can be performed in n_2 ways (regardless of how the first step was performed),

:

the k^{th} step can be performed in n_k ways (regardless of how the preceding steps were performed),
Then the entire operation can be performed in

$$n_1 \times n_2 \times n_3 \times \dots \times n_k \text{ ways}$$

Theorem 9.2.2 (Permutations)
The number of permutations of a set with $n \geq 1$ elements is n!

Theorem 9.2.3 (r-permutations from a set of n elem)
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

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

Theorem 9.3.1 (Addition Rule)
Suppose a finite set A equals the union of k distinct **mutually disjoint** subsets $A_1, A_2, \dots, A_k$. Then

$$|A| = |A_1| + |A_2| + \dots + |A_k|$$

Theorem 9.3.2 (Difference Rule)
If A is a finite set and $B \subseteq A$, then

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

Theorem 9.3.3 (Inclusion/Exclusion Rule)
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 PHP
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*

e.g., If 9 pigeonholes and 19 pigeons, at least one pigeonhole has 3 pigeons

Generalized PHP (Contrapositive)
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, $n \leq km$

e.g., If each pigeonhole has at most *k* pigeons, and there are *m* pigeonholes, then at most *km* pigeons in total

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

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

Theorem 9.5.2 (Permutation with indistinguishable)
Permutation with n total objects of which
n_1 are of type 1 and are indistinguishable
n_2 are of type 2 and are indistinguishable
:
n_k are of type k and are indistinguishable

suppose that $n_1 + n_2 + \dots + n_k = n$. Then the number of distinguishable permutations of the n objects is

$$\frac{n!}{n_1!\,n_2!\,n_3!\,\dots nk!}$$

Theorem 9.6.1 (r-combinations with repetition)
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

e.g., $x_1 + x_2 + x_3 = 20$, each x_i is a nonnegative integer. How many solution are there?
- each x is a category and each + is a partition
- think of it as how many ways to permutate 20 indistinguishable items and 2 indistinguishable partitions

Theorem 9.7.1 (Pascal's Formula)
Let n and r be positive integers, $r \leq n$. Then

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

Combinatorial Proof
Uses counting as the basis of the proof. It includes these types of proof:
1. Bijective proof. We have seen how to prove that two sets *X* and *Y* have the same cardinality by deriving a bijective function that maps each element in *X* to each element in *Y*.
2. Proof by double counting. Counting the number of elements in two different ways to obtain the different expressions in the identity

Theorem 9.7.2 (Binomial Theorem)
Given any real numbers a and b and any non-negative integer n,

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

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 events ($A \cap B = \emptyset$), then $P(A \cup B) = P(A) + P(B)$

Probability of General Union
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: 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 $p_1, p_2, p_3, \cdots, p_n$ respectively. The expected value of the process is

$$\sum_{k=1}^{n} a_k p_k = a_1 p_1 + a_2 p_2 + a_3 p_3 + \cdots + anp_n$$

Linearity of Expected Value
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* (which **may be dependent**),

$$E[X+Y] = E[X] + E[Y]$$

Definition: Conditional Probability
Let A and B be events in a sample space S. If $P(A) \neq 0$, then the conditional probability of B given A, denoted P(B|A), is

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

Theorem 9.9.1 (Bayes' Theorem)
Suppose that a sample space S is a union of mutually disjoint events $B_1, B_2, B_3, \dots, B_n$.
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

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

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

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

Graphs

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.

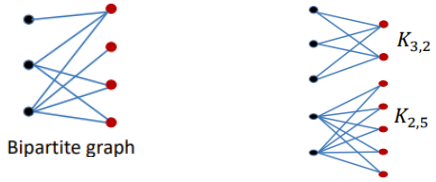
We write e = (v, w) for a directed edge e from vertex v to vertex w

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.)

Definition: Complete Graph
A complete graph on n vertices, n > 0, denoted K_n , is a simple graph with n vertices and exactly one edge connecting each pair of distinct vertices.
*total edges: nC2 (handshake) ; deg of each vertex: n-1

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 Vertex
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.

Definition: Total Degree of Undirected Graph
The total degree of G is the sum of the degrees of all the vertices of G

Theorem 10.1.1 (Handshake Theorem)
If G is any graph, then the sum of the degrees of all the vertices of G equals twice the number of edges of G. Specifically, if the vertices of G are v_1 , v_2 , …, v_n , where n ≥ 0, then
The **total degree** of G = $\deg(v_1) + \deg(v_2) + \dots + \deg(v_n) = 2 \times$ (**the number of edges** of G).

$$\sum_{v \in V} deg(v) = 2|E|$$

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. →use Q

Definition: Out/In degree of Vertex
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.

$$\sum_{v \in V} deg^-(v) = \sum_{v \in V} deg^+(v) = |E|$$

Definition: Walk & Trivial Walk
A **walk** from v to w is a finite alternating sequence of adjacent vertices and edges of G. Thus, a walk has the form

$$v_0\ e_1\ v_1\ e_2 \dots v_{n-1}\ e_n\ v_n ,$$

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.

Definition: Trail & Path
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

Definition: Closed walk, Circuit, Simple Circuit
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**

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.

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.

*A connected subgraph of largest possible size

Definition: Euler Circuit
Let G be a graph. An Euler circuit for G is a circuit that contains every vertex and traverses every edge of G exactly once.
*May visit vertexes more than once

Definition: Eulerian Graph
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.
*Converse not true

Theorem 10.2.2 (Contrapositive)
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.
*less strict than euler circuit (don't end at same vertex)

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.)
*does not need to include all edges; can repeat edges also

Definition: Hamiltonian Graph
A Hamiltonian graph (also called Hamilton graph) is a graph that contains a Hamiltonian circuit.

Hamiltonian vs Eulerian graph
Euler: Must include every vertex and traverse every edge exactly once (may visit vertex more than once)
Hamiltonian: include every vertex exactly once (does not need to include all edges)

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

for H, the subgraph

Contrapositive: If G does not have subgraph H with properties 1-4, then G does not have Hamiltonian circuit

Definition: Adjacency Matrix of Directed Graph
Let G be a directed graph with ordered vertices v_1, v_2, …, 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 Undirected Graph
Let G be a undirected graph with ordered vertices v_1, v_2, …, 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 from v_i to v_j
for all i, j = 1, 2, …, n.

Definition: Symmetric Matrix
An n × n square matrix A = (a_{ij}) is called symmetric if, and only if, $a_{ij} = a_{ji}$ for all i, j = 1, 2, …, n

Definition: Identity Matrix
Matrix with 1s in the main diagonal and 0s otherwise

Definition: nth 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
$\mathbf{A^n} = \mathbf{A} \times \mathbf{A^{n-1}}$ for all integers n ≥ 1

Theorem 10.3.2
If G is a graph with vertices v_1, v_2, …, 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 A^n = the number of walks of length n from v_i to v_j

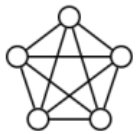
Definition: Isomorphic Graph
Let $G = (VG, EG)$ and $G' = (VG', EG')$ be two graphs. G is isomorphic to G', denoted $G \cong G'$, if and only if there exist bijections $g: V_G \to V_{G'}$ and $h: E_G \to E_{G'}$ that preserve the edge-endpoint functions of G and G' in the sense that for all $v \in V_G$ and $e \in E_G$,
v is an endpoint of $e \iff g(v)$ is an endpoint of $h(e)$

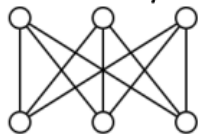
Theorem 10.4.1 (Graph Isomorphism Equiv Rel)
Let S be a set of graphs and let ≅ be the relation of graph isomorphism on S. Then ≅ is an equivalence relation on S.

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 $K_{3,3}$.

Subdivision: Take an edge and chop it into more edges (adding vertex)
*Thus, K_5 and $K_{3,3}$ are smallest non-planar graphs


K_5

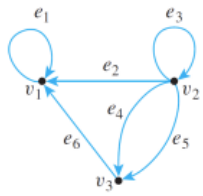

$K_{3,3}$

if smaller, auto planar. if not, try to switch and to check

Euler's Formula
For a connected planar simple graph G = (V, E) with e = |E| and v = |V|, if we let f be the number of faces, then
f = e – v + 2

Definition: Self-Complementary
A self-complementary graph is isomorphic with its complement

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)

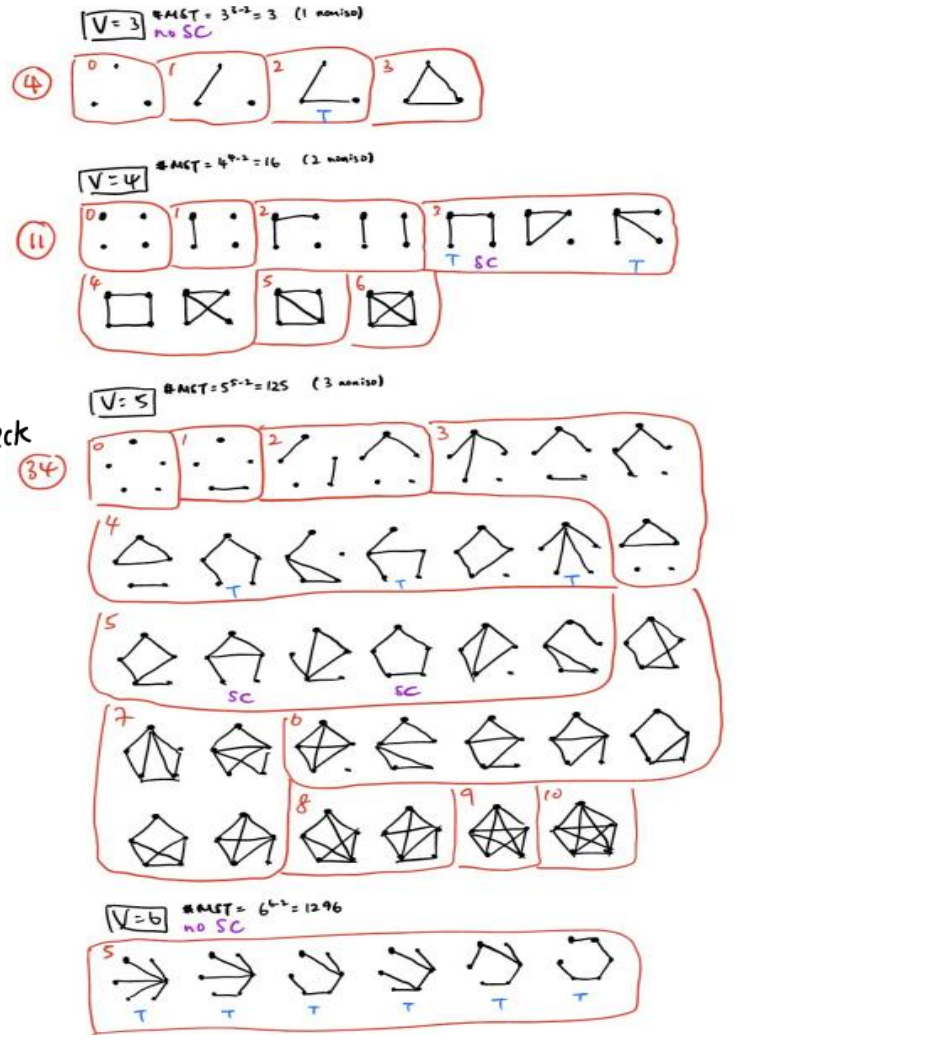


Directed Graph G

$$\mathbf{A} = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \end{array} \begin{array}{c} \begin{array}{ccc} v_1 & v_2 & v_3 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 2 \\ 1 & 0 & 0 \end{bmatrix} \end{array}$$
Adjacency Matrix

In a graph w/ 6 vertices; either G or $\overline{G}$ has a triangle
→ T1 09/12

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1k} \\ a_{21} & a_{22} & \cdots & a_{2k} \\ \vdots & \vdots & & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{ik} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mk} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1j} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2j} & \cdots & b_{2n} \\ & & & \cdot & & \\ & & & \cdot & & \\ & & & \cdot & & \\ b_{k1} & b_{k2} & \cdots & b_{kj} & \cdots & b_{kn} \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1j} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2j} & \cdots & c_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ c_{i1} & c_{i2} & \cdots & c_{ij} & \cdots & c_{in} \\ \vdots & \vdots & & \vdots & & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mj} & \cdots & c_{mn} \end{bmatrix}$$



Trees

Definition: Tree
(The graph is assumed to be undirected here.)
A **graph** is said to be **circuit-free** if and only if it has no circuits.
A simple graph is called a **tree** if and only if it is circuit-free and connected.
A **trivial tree** is a tree that consists of a single vertex.
A simple 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.
*non-trivial tree has a least two vertex of degree 1

Definition: Terminal Vertex 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.

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

Definition: 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

Definition: 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.

Definition: 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

Theorem 10.6.1 (Full Binary Tree)
If T is a full binary tree with k internal vertices, then T has a total of 2k + 1 vertices and has k + 1 terminal vertices (leaves).

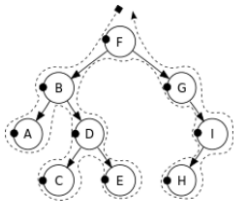
Theorem 10.6.2
For non-negative integers h, if T is any binary tree with height h and t terminal vertices (leaves), then

$t \leq 2^h$

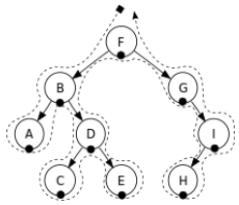
Equivalently,

$\log_2 t \leq h$

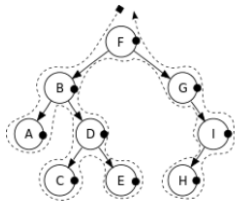
Depth First Search
- Pre-order
  - Print the **data** of the root (or current vertex)
  - Traverse the **left** subtree by recursively calling the pre-order function
  - Traverse the **right** subtree by recursively calling the pre-order function
- In-order
  - Traverse the **left** subtree by recursively calling the in-order function
  - Print the **data** of the root (or current vertex)
  - Traverse the **right** subtree by recursively calling the in-order function
- Post-order
  - Traverse the **left** subtree by recursively calling the post-order function
  - Traverse the **right** subtree by recursively calling the post-order function
  - Print the **data** of the root (or current vertex)



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
1. Every connected graph has a spanning tree.
2. Any two spanning trees for a graph have the same number of edges

Definition: Weighted Graph
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.

Definition: Minimum Spanning Tree
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
Examine edges in increasing weight. The edge being examined is being added to what will become the minimum spanning tree, provided that this addition does not create a circuit. When n

Prim's Algorithm
Start with a vertex. Choose an edge that connect to a new vertex and has the least weight of all edges connecting to a new vertex. Repeat.

Number of Isomorphic tree
Number of isomorphic tree for n vertex = n^{n-2}

Finding non-isomorphic tress of n vertices
- By T10.5.2, tree with n vertices has n-1 edges
- By handshake theorem, total degree = 2(n-1)
- Every non-trivial tree has ≥ 2 vertices of degree 1
- find the combinations of degrees for the n vertices and draw out the trees

Tutorial Proofs

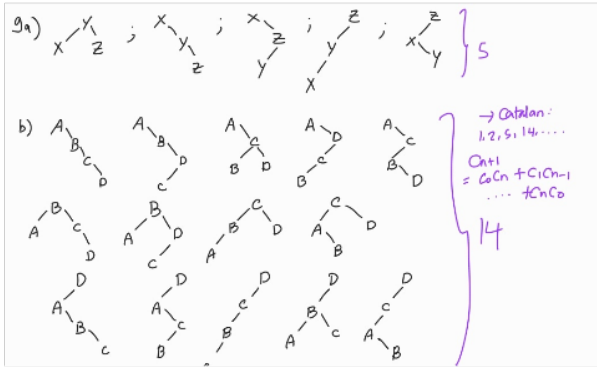
Proof (~~Tutorial 11 Q2~~) somewhere?
For any simple planar graph with *f* faces, *v* vertices and *e* edges ($e \geq 2$) ,
a. $3f \leq 2e$
b. $e \leq 3v - 6$.

Proof (Tutorial 11 Q5)
G is simple, undirected graph. If G connected, then $|E| \geq |V| - 1$.
Converse not true.

Proof (Tutorial 11 Q6)
G is simple, undirected graph. If G acyclic, then $|E| \leq |V| - 1$
Converse not true.

Proof (Tutorial 11 Q7)
G is simple, undirected graph. G is a tree iff there is exactly one path between every pair of vertices.

All possible binary trees w/ n vertices:
Catalan's: 1, 2, 5, 14, ..



Bipartite only when total deg divisible by 2.
For complete; $2 \mid \frac{n(n-1)}{2} \rightarrow 4 \mid n$ or $4 \mid n-1$

Every simple planar graph has a degree of at most 5.

Misc

Definition (Even and Odd Integers)
n is even $\Leftrightarrow \exists$ an integer k such that $n = 2k$.
n is odd $\Leftrightarrow \exists$ an integer k such that $n = 2k + 1$

Definition: Divisibility
Let $n, d \in \mathbb{Z}$. Then $d \mid n \Leftrightarrow n = dk$ for some $k \in \mathbb{Z}$.

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 $a \mid b$

Definition (Prime and Composite number)
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

n is prime $\Leftrightarrow$
$\forall r, s \in Z^+$ n = rs $\rightarrow$ (r = 1 $\wedge$ s = n) $\vee$ (r = n $\wedge$ s = 1)

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.

n is composite $\Leftrightarrow$
$\exists r, s \in Z^+$ s.t. n = rs $\wedge$ (1 < r < n) $\wedge$ (1 < s < n)

Definition (Rational Numbers)
r is rational $\Leftrightarrow \exists$ integers a and b such that $r = \frac{a}{b}$ and $b \neq 0$

Theorem 4.4.1 (Quotient-Remainder Theorem)
Given any integer n and positive integer d, there exist unique integers q and r such that

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

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.

Corollary 4.2.3 (5th: 4.2.3)
The double of a rational number 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|b, then a ≤ b.

Theorem 4.3.2 (5th: 4.4.2) Divisors of 1:
The only divisors of 1 are 1 and -1.

Theorem 4.6.1 (5th: 4.7.1)
There is no greatest integer.

Theorem 4.6.4 (5th: 4.7.4)
For all integers n, if n^2 is even then n is even

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

Proof (Tutorial 1 Q10)
The product of any two odd integers is an odd integer

Proof (Tutorial 1 Q11)
n^2 is odd if and only if n is odd.

Proof (Tutorial 2 Q4(a))
Integers are not closed under division.

Proof (Tutorial 2 Q4(b))
Rational numbers are closed under addition.

Proof (Tutorial 2 Q4(c))
Rational numbers are not closed under division.

Proof (Tutorial 2 Q8)
$\forall x \in R((x\ 2 > x) \rightarrow (x < 0) \vee (x > 1))$.

Proof (Tutorial 2 Q11)
If n is a product of two positive integers a and b, then a ≤ $n^{1/2}$ or b ≤ $n^{1/2}$

Proof (Tutorial 3 Q3(a))
There exist non-empty finite sets A and B such that $|A \cup B| = |A| + |B|$

Proof (Tutorial 3 Q3(b))
There exist non-empty finite sets A and B such that $|A \cup B| \neq |A| + |B|$

Proof (Tutorial 3 Q5)
$A \cap (B \setminus C) = (A \cap B) \setminus C$

Proof (Tutorial 3 Q8)
$A \subseteq B$ if and only if $A \cup B = B$

Exclusive-Or for Sets (Tutorial 3 Q7)
In A or B but not both:

$$A \oplus B = (A \setminus B) \cup (B \setminus A)$$
$$A \oplus B = (A \cup B) \setminus (A \cap B)$$

Properties of Integers
1. **Closure**: under addition and multiplication
2. **Commutative**: for addition and multiplication
3. **Associative**: for addition and multiplication
4. **Distributive**: Multiplication is distributive over addition but not other way round
5. **Trichotomy**: exactly one of the following is true, x = y, or x < y or x > y

***Additional Integer properties (Do not quote)**
n^2 is even if and only if n is even
Sum of two odd integers is even
Sum of two even integers is even
Sum of even and odd is odd

Bell's Number (num of partitions for n element-set)
1, 1, 2, 5, 15, 52, 203, 877, 414021147, 115975,…

Proof Types

- By **Construction**: finding or giving a set of directions to reach the statement to be proven true. In proving equality, a useful note:

$$a \leq b \wedge a \geq b \Rightarrow a = b$$

- By **Contraposition**: proving a statement through its logically equivalent contrapositive.

- By **Contradiction**: assuming that the negation of the statement is true, which then leads to a logical contradiction.

- By **Cases**: List out the general cases and prove that statement holds in every general case

- By **Exhaustion**: considering all cases

- By **Mathematical Induction**: proving for a base case, then an induction step. In the inductive step, work from the k + 1, not the k case.

- By **Strong Induction**: mathematical induction assuming P (k), P (k − 1), · · · , P (a) are all true.

Proof Technique
When asked to prove 3 statements (i), (ii), (iii) are logically equivalent,
- Prove (i) ⇒ (ii)
- Prove (ii) ⇒ (iii)
- Prove (iii) ⇒ (i)

Past Midterm Notes

- When proving/disproving, don't forget about <-> = both ways
- Take note of words like **unique, different, only if, etc.**
- Absorption law is **underused**
- Don't immediately expand a logical statement: consider adding a universal statement like or ...$\wedge(p \vee \sim p)$
- Pay attention to definitions of sets and orders **especially with comparisons.**
- e.g. May be true for x < y but is it true for x > y?
- Try to take shortcuts through stuff learnt in tutorials.
- Introduce universal/existential statments only when required. Try to not dump variables all at the start.
- Order of variables in universeal/existential statements **matter**. Best way is to try to interpret them in English.
- Always **double** check for **transitivity**! Not all elements need reflexivity in transitivity.
- Argument is **unsound** = premises are not all true. ==> argument is vacuously valid
- Only **invalid** if premises are all true but conclusion is not true.

Any relation on $\emptyset$:
- Reflexive
- Irreflexive
- Transitive
- Symmetric
- Antitransitive
- Antisymmetric
- Asymmetric

A relation $R = \{\}$ on a non-empty A:
- Not reflexive
- Irreflexive
- Symmetric
- Antisymmetric
- Asymmetric
- Transitive
- Antitransitive

Asymmetry $\Leftrightarrow$ Irreflexive and Antisymmetry

Any element in R where R is transitive or symmetric; xRx
! but not the elements not R-related to anything

Don't forget of xRx only in posets!
They are both maximal & minimal
& any part ord is REFLEXIVE

Break down absolutes in universal or existential statements.
↳ taker shorter than you'd expect.

- $P(A \cap B) = P(A) \cap P(B)$
  but $P(A \cup B) \neq P(A) \cup P(B)$
- Well-ordered set:
  all non-$\emptyset$ subsets have smallest els;
  including infinite subsets.
- Generally, no other relations between refl, asymm, antisym, symm, trans, or antitrans.
  ↳ most $\leftrightarrow$ can be broken by counter e.g.
- R reflexive $\wedge$ S symmetric.
  $\therefore$ RUS is reflexive.
  ★always consider how 2 relations involve entirely different elements.
- $R \circ R = R$
  $R = R^{-1}$
  $R \circ R^{-1} = R^{-1} \circ R$
  and any other corresponding formula
  } for R is an equ reltn T4Q5
- Binary relation $\subseteq$ on R is a partial order.
  (Tutorial 5 Qn. 5)
- $(p \to q) \wedge (q \to r)$
  $p \to r$
  } valid
  but $(p \to q) \to r \not\equiv p \to (q \to r)$ by T1Q4
- $(a \to b) \wedge (a \to c) \to (a \to (b \vee c))$
  $(a \to b) \wedge (a \to c) \to (a \to (b \wedge c))$
  } both true.

The real numbers also satisfy the following axioms, called the **order axioms**. It is assumed that among all real numbers there are certain ones, called the **positive real numbers**, that satisfy properties Ord1, Ord2, and Ord3.

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.

The symbols $<$, $>$, $\leq$, and $\geq$, and negative numbers are defined in terms of positive numbers.

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**.

From the order axioms Ord1, Ord2, and Ord3 and the above definition, all the usual rules for calculating with inequalities can be derived. The most important are collected as theorems T17, T18, T19, T20, T21, T22, T23, T24, T25, T26, and T27 as follows. In all these theorems the symbols a, b, c, and d represent arbitrary real numbers.

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 $0 < ab < cd$.

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

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

T1. *Cancellation Law for Addition* If $a+b=a+c$, then $b=c$. (In particular, this shows that the number 0 of Axiom F4 is unique.)

T2. *Possibility of Subtraction* Given a and b, there is exactly one x such that $a+x=b$. This x is denoted by $b-a$. In particular, $0-a$ is the additive inverse of a, $-a$.

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*

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

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*

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

More Past Finals Notes

- $A \times (B \cup C) = (A \times B) \cup (A \times C)$
- $A \times (B \cap C) = (A \times B) \cap (A \times C)$
- $a \equiv b \bmod n \rightarrow ac \equiv bc \bmod n$
  but not converse!
- R refl, symm, trans $\rightarrow$ R^{-1} refl, R^{-1} symm, R^{-1} trans
- if $|A| = |B|$; $f: A \to B$ not inj $\Leftrightarrow$ not surj
- $\forall n \in \mathbb{N}_{\geq 2}$; $\exists a \in \mathbb{Z}^+$ s.t. $a, a+1, a+2, \ldots a+n$ } composite
  $a = (n+2)! + 2$
  $a+1 = (n+2)! + 3$
  $\vdots$
  $a+k = (n+2)! + k+2 = (k+2)\left(1 + \frac{(n+2)!}{k+2}\right)$ } alw comp for $k = 1, 2, \ldots n$
- $a \equiv b \bmod n$, $c \equiv d \bmod n$ $\rightarrow$ $a+c \equiv b+d \bmod n$, $ac \equiv bd \bmod n$
- Drawing possible trees:
  - Find total degree
  - Any conditions: root? binary?
    e.g. min 2 vertices w/ degree 1 for non-trivial tree
  - Find combos
    ↳ use Catalan w/ appl for full binary
    ↳ refer to graphs in CS
- Catalan: for distinct full binary trees
- 1, 1, 1, 2, 3, 6, 11, 23, ... No of unlabeled trees in general → from Tut & PYP. (& isom.)
- n^{n-2} = No of labeled trees in general (isomorphic)
- 1, 1, 2, 4, 9, 20, 48, ... No of unlabeled isom rooted trees
- n^{n-1} = No of labeled, rooted trees (isomorphic)
- $f = id_A \Leftrightarrow g \circ f = g$ for inj/surj fctn g; OR $id_A \circ f = id_A$ $(f: A \to A)$
- Set $\mathbb{Z}^*$ of all strings over $\mathbb{Z}$ is countable.
- Injective: $|B| \geq |A|$; Surjective: $|A| \leq |B|$
- 'Bipartite graph' very loose! can include empty/near-empty
- $A \subsetneq B$: $P(A) \leq P(B)$ & $P(\bar{A}) \geq P(\bar{B})$
- For symbols: $=$; $\subseteq$; $\neq$ check for all cases, not just in certain ones.
- f, g inj/surj/bij $\rightarrow$ $f \circ g$ inj/surj/bij but not converse
- Bell number: No. of equiv rltns w/ n els: $1^0, 1^1, 2^2, 5^3, 15^4, 52, \ldots$
  also, no. of partitions w/ n els: $B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k$