CS1231

Proof Techniques:

Direct, Contrapositive, Induction & Strong Induction, Contradiction

Propositional Logic:

Impt Tables:

1	Commutative laws	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
2	Associative laws	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
3	Distributive laws	$p \wedge (q \vee r)$ $\equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r)$ $\equiv (p \vee q) \wedge (p \vee r)$
4	Identity laws	$p \wedge \mathbf{t} \equiv p$	$p \vee \mathbf{c} \equiv p$
5	Negation laws	$p \vee {\sim}p \equiv \mathbf{t}$	$p \wedge {\sim}p \equiv \mathbf{c}$
6	Double negative law	${\sim}({\sim}p) \equiv p$	
7	Idempotent laws	$p \wedge p \equiv p$	$p \vee p \equiv p$
8	Universal bound laws	$p \vee \mathbf{t} \equiv \mathbf{t}$	$p \wedge \mathbf{c} \equiv \mathbf{c}$
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 **t** and **c**	${\sim}\mathbf{t} \equiv \mathbf{c}$	${\sim}\mathbf{c} \equiv \mathbf{t}$

Importance of Operations:

NOT>(AND=OR)>(IMPLIES==IF AND ONLY IF (BICONDITIONAL))

Valid and Invalid Arguments:

Rule of inference		
Modus Ponens	$p \rightarrow q$ p $\bullet\ q$	
Modus Tollens	$p \rightarrow q$ ${\sim}q$ $\bullet\ {\sim}p$	
Generalization	p $\bullet\ p \vee q$	q $\bullet\ p \vee q$
Specialization	$p \wedge q$ $\bullet\ p$	$p \wedge q$ $\bullet\ q$
Conjunction	p q $\bullet\ p \wedge q$	

Rule of inference		
Elimination	$p \vee q$ ${\sim}q$ $\bullet\ p$	$p \vee q$ ${\sim}p$ $\bullet\ q$
Transitivity	$p \rightarrow q$ $q \rightarrow r$ $\bullet\ p \rightarrow r$	
Proof by Division Into Cases	$p \vee q$ $p \rightarrow r$ $q \rightarrow r$ $\bullet\ r$	
Contradiction Rule	${\sim}p \rightarrow c$ $\bullet\ p$	

DEFINITIONS:

Divisibility (Definiton 1.3.1):

If n and d are integers and d≠ 0

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

i.e. $d|n \Leftrightarrow \exists\ integer\ k\ such\ that\ n = dk\ and\ d \neq 0$

Even and Odd Numbers (Definition 1.6.1):

An integer as even iff it is twice some other integer. It is odd iff it is twice some other integer+1

$n \text{ is even} \Leftrightarrow \exists \text{ integer } k \text{ such that } n = 2k$

$n \text{ is odd} \Leftrightarrow \exists \text{ integer } k \text{ such that } n = 2k + 1$

Prime Numbers (Definition 4.2.1):

An integer n is prime or composite according to the following:

$n \text{ is prime} \Leftrightarrow n > 1 \text{ and } \forall\, r, s \in \mathbb{Z}^+, \text{if } n = rs \text{ then } (r = 1 \text{ and } s = n)\ OR\ (r = n \text{ and } s = 1)$
$n \text{ is composite} \Leftrightarrow n > 1 \text{ and } \exists\, r, s \in \mathbb{Z}^+ \text{ such that } n = rs \text{ and } 1 < r, s < n$

Lower Bound:

$\text{An integer } b \text{ is said to be a lower bound for a set } X \subseteq \mathbb{Z} \text{ if } b \leq x,\ \forall x \in X$

Greatest Common Divisor (Definition 4.5.1):

$\text{Let } a \text{ and } b \text{ not both zero integers.}$
$\text{The greatest common divisor of } a \text{ and } b (\text{denoted } \gcd(a, b)), \text{is the integer } d \text{ which satisfies the following}$

$(i) d|a \text{ and } d|b \text{ and } (ii) \forall c \in \mathbb{Z} \text{ if } c|a \text{ and } c|b \text{ then } c \leq d]$

Co-prime (Definition 4.5.3):

$\text{Integers } a \text{ and } b \text{ are } co - prime \Leftrightarrow \gcd(a, b) = 1$

Least Common Multiple (Definition 4.6.1):

$\text{An integer } m = lcm(a, b) \text{where } a, b \text{ are not both zero is defined such that}$

$(i) a|m \text{ and } b|m\ (ii) \text{for all integers } c, \text{if } a|c \text{ and } b|c \text{ then } m \leq c.$

Modular congruence (Definition 4.7.1):

$\text{Let } m \& n \text{ be integers, and let } d \text{ be a positive integer. We say that } m \text{ is congruent to } n \text{ modulo } d \text{ and write}$

$m \equiv n (mod\ d),\ \text{if and only if } d|(m - n)$

Multiplicative inverse modulo n (Definition 4.7.2):

$\text{For any integers } a, n \text{ with } n > 1, \text{if an integer } s \text{ is such that } as \equiv 1\ (mod\ n),$

$\text{then } s \text{ is called the } \boldsymbol{\text{multiplicative inverse of } a \text{ modulo } n}.$
$\text{We may write it as } a^{-1}. \text{Also note that } a^{-1}a \equiv 1\ (mod\ n) \text{ due to commutativity}$

Second-order Linear Homogeneous Recurrence Relation with Constant Co-efficients:

$\text{The above is defined as a recurrence relation with the form:}$

$a_k = Aa_{k-1} + Ba_{k-2}, \forall k \in \mathbb{Z}_{\geq k_0},$

$\text{where } A, B \text{ are real constants and } B \neq 0 \text{ and } k_0 \text{ is an integer constant}$

Set Theory Definitions:

Empty Set (Definition 6.3.1):

$The\ empty\ set\ has\ no\ element\ and\ is\ denoted\ by\ \phi\ or\ \{\ \}.$

Set Equality (Definition 6.3.2):

$Two\ sets\ are\ equal\ iff\ they\ have\ the\ same\ elements:$

$i.e. \forall X \forall Y((\forall Z(Z \in X \longleftrightarrow Z \in Y)) \longleftrightarrow X = Y)$

Power Set (Definition 6.3.4):

$Given\ any\ set\ S, the\ power\ set\ of\ S\ denoted\ as\ \mathcal{P}(S)\ or\ 2^S, is\ the\ set\ whose\ elements\ are\ all\ subsets\ of$ $the\ set\ S, nothing\ less\ and\ nothing\ more.$

$i.e. If\ T = \mathcal{P}(S), then\ \forall X((X \in T) \longleftrightarrow (X \subseteq S))$

Union (Definition 6.4.1):

$Let\ S\ be\ a\ set\ of\ sets. We\ say\ T\ is\ the\ union\ of\ all\ sets\ in\ S\ iff\ each\ element\ in\ T\ belongs\ to\ some\ set\ in\ S$ $nothing\ less, nothing\ more. We\ write\ it\ as\ such:$

$$T = \bigcup S = \bigcup_{X \in S} X\ \ such\ that\ \forall Y\left((Y \in T) \longleftrightarrow \exists Z\big((Z \in S) \land (Y \in Z)\big)\right)$$

Intersection (Definition 6.4.3):

$Let\ S\ be\ the\ set\ of\ nonempty\ sets.\ We\ say\ T\ is\ the\ intersection\ of\ all\ sets\ in\ S\ iff\ each\ element\ in\ T$ $belongs\ to\ all\ the\ sets\ in\ S, nothing\ less, nothing\ more. We\ write\ it\ as\ such:$

$$T = \bigcap S = \bigcap_{X \in S} X\ such\ that\ \forall Y((Y \in T) \leftrightarrow \forall Z\big((Z \in S) \to (Y \in Z)\big))$$

Disjoint Sets (Definition 6.4.5):

$Two\ sets\ S\ and\ T\ are\ disjoint\ iff\ S \cap T = \phi$

Mutually Disjoint (Definition 6.4.6):

$Let\ V\ be\ a\ set\ of\ sets. The\ sets\ T \in V\ are\ said\ to\ be\ mutually\ disjoint\ iff:$

$\forall X, Y \in V(X \neq Y \to X \cap Y = \phi)$

Partition (Definition 6.4.7):

$Let\ S\ be\ set\ , and\ let\ V\ be\ a\ set\ of\ nonempty\ subsets\ of\ S. V\ is\ partition\ iff:$

$(i) V\ is\ mutually\ disjoint\ and\ (ii) \bigcup V = S$

Non-symmetric difference (A-B) (Definition 6.4.8):

$A - B\ is\ defined\ as\ elements\ that\ are\ in\ A\ but\ not\ in\ B, nothing\ less\ nothing\ more.$

$$i.e. \forall X\big(X \in (A - B) \leftrightarrow (X \in A \land X \notin B)\big)$$

Symmetric-Difference (Definition 6.4.9):

$The\ symmetric\ difference\ (A \ominus B) is\ defined\ as\ elements\ that\ are\ in\ A\ or\ in\ B\ but\ not\ both$

$\forall X\left(X \in (A \ominus B) \leftrightarrow \left((X \in A) \oplus (X \in B)\right)\right)$

Complement (Definition 6.4.10):

$Let\ \mathcal{U}\ be\ the\ Universal\ Set\ where\ A \subseteq U. Then\ the\ complement\ A^c, is\ \mathcal{U} - A$

Cartesian product (Definition 8.1.3 &8.1.4 (general)):

$Let\ S\ and\ T\ be\ two\ sets. Their\ Cartesian\ product, written\ as\ S \times T\ is\ defined\ as:$

$\forall X \forall Y\big((X, Y) \in S \times T \leftrightarrow (X \in S \land Y \in T)\big). It\ is\ not\ commutative\ or\ associative.$

$Generalizing\ for\ n\ sets\ it\ can\ be\ represented\ as\ the\ sets\ S\ in\ V\ :$

$$\prod_{S \in V} S$$

Relation (Definition 8.2.1 & 8.2.7(generalized))

$For\ any\ two\ sets\ S\ and\ T, a\ binary\ relation\ \mathcal{R}\ from\ S\ to\ T\ is\ \ subset\ of\ S \times T. Therefore:$

$x\ \mathcal{R}\ y \rightarrow (x, y) \in S \times T$

$x\ \not\mathcal{R}\ y \rightarrow (x, y) \notin S \times T$

$Can\ be\ generalized\ to\ n - ary\ relation, where\ n\ is\ the\ arity/degree\ of\ the\ relation$

Domain, Range, Co-domain (Definition 8.2.2 to 8.2.4):

$For\ any\ binary\ relation\ from\ S\ to\ T:$

$Domain = \{s \in S | \exists t \in T(s\ \mathcal{R}\ t)\}, Codomain = T, Range/Image = \{t \in T | \exists s \in S(s\ \mathcal{R}\ t)\}$

$Therefore\ Range \subseteq Codomain$(**Proposition 8.2.5)**

Inverse Relation (Definition 8.2.6):

$The\ inverse\ relation\ \mathcal{R}^{-1}\ from\ T\ to\ S\ is\ such\ that:$

$\forall s \in S, \forall t \in T(t\ \ \mathcal{R}^{-1}\ s \leftrightarrow s\ \mathcal{R}$ t)

Composition (Definition 8.2.9):

$For\ the\ three\ sets\ S, T\ \&U, let\ a\ relation\ \mathcal{R}\ be\ from\ S\ to\ T\ and\ a\ relation\ \mathcal{R}'be\ from\ T\ to\ U.$

$The\ composition\ of\ that\ relation\ \mathcal{R}' \circ \mathcal{R}\ is\ such\ that\ \mathcal{R}' \circ \mathcal{R} \subseteq S \times U\ and:$

$\forall x \in S, \forall z \in U(x\ \mathcal{R}' \circ \mathcal{R}\ z \leftrightarrow \Big(\exists y \in T\big((x\ \mathcal{R}\ y) \land (y\ \mathcal{R}\ z)\big)\Big)$

Reflexivity, Symmetry and Transitivity of Relations (8.3.1 to 8.3.3):

$The\ following\ are\ used\ to\ describe\ relations\ on\ a\ set\ A\ and\ itself:$

$(8.3.1) Reflexive: \forall x \in A(x\ \mathcal{R}\ x) \leftrightarrow \mathcal{R}\ is\ reflexive.$

$Irreflexive: \mathcal{R}\ is\ irreflexive\ \forall x \in A\ (x\ \not\mathcal{R}\ x)$

$(8.3.2) Symmetric: \mathcal{R}\ is\ symmetric \leftrightarrow \forall x, y \in A(x\ \mathcal{R}\ y \rightarrow y\ \mathcal{R}\ x)$

$(8.6.1) Anti - symmetric: \mathcal{R}\ is\ anti - symmetric \leftrightarrow \forall x, y \in A(x\ \mathcal{R}\ y \land y \mathcal{R} x \rightarrow x = y)$

$Asymmetric: \mathcal{R}\ is\ asymmetric \leftrightarrow \forall x, y \in A(x\ \mathcal{R}\ y \rightarrow y \not\mathcal{R}\ x)$

$i.e. \mathcal{R}\ is\ antisymmetric\ and\ irreflexive$

(8.3.3)$Transitive: \mathcal{R}\ is\ transitive \leftrightarrow \forall x, y, z \in A\ ((x\ \mathcal{R}\ y \wedge y\ \mathcal{R}\ z) \rightarrow x\ \mathcal{R}\ z)$

Definition 8.3.4 (Equivalence Relation):

$If\ a\ relation\ \mathcal{R}\ on\ A\ is\ reflexive, transitive\ and\ symmetric, \mathcal{R}\ is\ said\ to\ be\ an\ equivalence\ relation$

Definition 8.3.5 (Equivalence Class):

$Let\ \mathcal{R}\ be\ an\ equivalence\ relation$

$Let\ x \in A. The\ equivalence\ class\ of\ x\ , denoted\ as\ [x], is\ the\ set\ of\ all\ y \in A\ such\ that\ x\ \mathcal{R}\ y:$

$i.e. [x] = \{y \in A | x\ \mathcal{R}\ y\}$

Definition 8.5.1 (Transitive Closure):

$Let\ \mathcal{R}\ be\ a\ relation\ on\ set\ A. The\ transitive\ closure\ of\ \mathcal{R}, denoted\ as\ \mathcal{R}^t, is\ a\ relation\ that\ satisfies\ the$

$the\ following:$

(1)$It\ is\ transitive,$ (2)$\mathcal{R} \subseteq \mathcal{R}^t,$ (3)$For\ any\ transitive\ relation\ \mathcal{S}\ on\ A, where\ \mathcal{R} \subseteq \mathcal{S}, \mathcal{R}^t \subseteq S$

Definition 8.6.2 (Partial Order):

$\mathcal{R}\ is\ said\ to\ be\ a\ partial\ order\ iff\ it\ is\ reflexive, antisymmetric\ and\ transitive. Partial\ orders\ are$

$denoted\ by \preccurlyeq. A\ is\ poset\ if \preccurlyeq is\ a\ partial\ order\ relation\ on\ A.$

Definition 8.6.3 (Comparable):

$Let \preccurlyeq be\ partial\ order\ relation\ on\ A. For\ a, b \in A\ \ are\ said\ to\ be\ comparable\ iff\ a \preccurlyeq b$

$or\ b \preccurlyeq a. If\ no\ such\ relation\ exists\ between\ a\ and\ b, the\ are\ said\ to\ be\ noncomparable$

Definition 8.6.4 (Total Order):

$If \preccurlyeq is\ a\ partial\ order\ on\ set\ A, \preccurlyeq is\ a\ \textbf{total order}\ iff:$

$\forall a, b \in A(a \preccurlyeq b \vee b \preccurlyeq a). i.e. All\ elements\ in\ A\ are\ comparable\ to\ each\ other$

Definitions 8.6.5-8.6.8 (Minimax definitions):

8.6.5 $Maximal: An\ element\ b \in A\ is\ said\ to\ be\ \textbf{maximal element}\ iff\ \forall c \in A(b \preccurlyeq c \rightarrow b = c)$

8.6.7 $Minimal: An\ element\ a \in A\ is\ a\ \textbf{minimal element}\ \ iff\ \forall b \in A(b \preccurlyeq a \rightarrow b = a)$

$(Note\ vacuous\ truth\ for\ non\ comaparable\ elements. Same\ hold\ for\ maximal)$

8.6.6 $Maximum: An\ element\ \top \in A\ is\ said\ to\ be\ the\ \textbf{maximum}\ iff\ \forall y \in A\ (y \preccurlyeq \top)$

8.6.8 $Minimum: An\ element\ \bot \in A\ is\ said\ to\ be\ the\ \textbf{minimum}\ iff\ \forall y \in A(\bot \preccurlyeq y)$

$(Note\ minimum/maximum\ requires \preccurlyeq to\ be\ a\ total\ order)$

Definition 8.6.9.

$Let \preccurlyeq\ be\ a\ total\ order\ on\ A.\ Iff\ every\ nonempty\ subset\ of\ A\ contains\ a\ minimum\ element,$

$A\ is\ said\ to\ be\ well\ ordered. Formally: \forall S \in \mathcal{P}(A)(S \neq \phi \rightarrow (\exists x \in S(\forall y \in S(x \preccurlyeq y))))$

Definition 7.1.1 (Function):

$Let\ f\ be\ a\ relation\ from\ S\ to\ T. f\ is\ a\ function\ from\ S\ to\ T\ iff\ \forall x \in S\big(\exists!\, y \in T\ (x\ f\ y)\big)$

Definition 7.1.2-7.1.5:

$Let\ f\ be\ a\ function\ from\ S\ to\ T$

7.1.2 $x\ is\ the\ pre-image\ for\ y\ if\ f(x) = y$

7.1.3 $The\ inverse\ image\ of\ y = \{x \in S | f(x) = y\}$

7.1.4 $For\ any\ U \subseteq T, the\ inverse\ image\ of\ U\ is\ the\ set\ of\ all\ inverse\ images\ of\ y \in U.$

7.1.5 $The\ restriction\ of\ f\ to\ U \subseteq S\ is\ the\ set : \{\,(x, y) \in U \times T | f(x) = y\}$

Definition 7.2.1-7.2.3(Injective, Surjective, Bijective, Identity):

7.2.1 $Let\ f\ be\ a\ function\ from\ S\ to\ T. f\ is\ injective/f\ is\ one\text{-}to\text{-}one/\ f\ is\ an\ injection\ iff$:

$$\forall y \in T\ , \forall x_1, x_2 \in S((f(x_1) = y \land f(x_2) = y) \rightarrow\ x_1 = x_2$$

7.2.2 $Let\ f\ be\ a\ fucntion\ from\ S\ to\ T. f\ is\ surjective/f\ is\ onto/f\ is\ a\ surjection\ iff$:

$$\forall y \in T, \exists \in S(f(x) = y)$$

7.2.3 $A\ function\ is\ bijective\ iff\ it\ is\ injective\ and\ surjective. We\ call\ such\ an\ f\ a\ bijection$

7.3.2 $The\ identity\ function\ (\mathcal{I}_A)\ on\ A\ from\ A\ is\ defined\ as\ \forall x \in A(\mathcal{I}_A(x) = x)$

Counting and Probability:

Sample Space:

$A\ sample\ space, S\ is\ the\ set\ of\ all\ possible\ event\ outcomes\ of\ a\ random\ \ process\ or\ experiment.$

$An\ event, E\ is\ the\ susbet\ of\ the\ sampel\ space.$

Probability:

$For\ a\ finite\ sample\ space, S\ in\ which\ all\ outcomes\ are\ equally\ likely\ and\ E\ is\ an\ event\ in\ S, then$

$the\ probability\ of\ E\ occurring\ is : P(E) = \dfrac{The\ number\ of\ outcomes\ in\ in\ E}{The\ number\ outcomes\ in\ S} = \dfrac{N(E)}{N(S)}$

r-Combinations:

Let *n* and *r* be non-negative integers with *r* ≤ *n*.

An *r*-combination of a set of *n* elements is a subset of *r* of the *n* elements.

Expected Value:

$Suppose\ events\ a_1, a_2, a_3 .. a_k\ occur\ with\ probabilities\ p_1, p_2, p_3 .. p_k. Then\ the\ expected\ value\ of$

$of\ this\ process\ is: \displaystyle\sum_{i=1}^{k} a_i \cdot p_i$

Conditional probability:

$Given\ two\ events\ A\ and\ B\ in\ sample\ space\ S. If\ P(A) \neq 0, then\ conditional\ probability$

$of\ B\ given\ A, written\ as\ P(B|A) = \dfrac{P(A \cap B)}{P(A)}$

Independent Events:

$If\ A\ and\ B\ are\ events\ in\ a\ sample\ space\ S, then\ A\ and\ B\ are\ independent\ iff:$

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

Pairwise Independent:

$Events\ A, B\ and\ C\ in\ a\ sample\ space\ S\ are\ pairwise\ independent, if\ 1-3\ are\ satisfied.$

$If\ 4\ is\ satisfied, they\ are\ said\ to\ be\ mutually\ independent.$

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

$\boldsymbol{Note}: \boldsymbol{Pairwise\ and\ mutual\ independence\ are\ unrelated. One\ doesn't imply\ the\ other}.$

GRAPH THEORY:

Graph:

$A\ graph\ G\ consists\ of\ two\ finite\ sets: A\ nonempty\ set\ of\ vertices\ V(G)\ and\ a\ set\ of\ edges\ E(G),$

$where\ each\ edge\ is\ associated\ with\ two\ vertices\ called\ its\ endpoints.$

$If\ an\ edge\ connects\ 2\ vertices, they\ are\ said\ to\ be\ adjacent, even\ if\ it\ is\ a\ self\ loop.$

$Edges\ incident\ on\ the\ same\ endpoint\ are\ said\ to\ be\ adjacent\ as\ well.\ \ An\ edge\ e\ with\ endpoints$

$v\ and\ w\ are\ represented\ as\ given: e = \{v, w\}$

$\boldsymbol{Directed}: If\ a\ graph\ G\ is\ directed, the\ edges\ set\ is\ now\ a\ set\ of\ \boldsymbol{ordered\ pairs}\ D(G). If\ the\ edges$

$goes\ from\ v\ to\ w, the\ directed\ edge\ is\ represented\ as\ e = (v, w)$

$\boldsymbol{Simple}: A\ simple\ grpah\ has\ no\ parallel\ edges\ or\ self\ loops$

$\boldsymbol{Complete}: A\ complete\ graph\ with\ n\ vertices, is\ a\ simle\ graph\ where\ each\ vertex\ is\ adjacent\ to\ an$

$other\ vertex\ in\ the\ vertex\ set.$

$\boldsymbol{Complete\ Bipartite}: A\ bipartite\ graph\ , denoted\ K_{m,n}, is\ a\ complete\ graph\ with\ two\ disjoint\ vertex\ sets$

$of\ m\ and\ n\ vertices\ respectively. Note\ that\ there\ will\ be\ no\ edge\ connecting\ two\ vertices\ of\ the\ same\ set$

$but\ there\ will\ be\ one\ edge\ between\ each\ and\ every\ vertex\ in\ set\ 1\ to\ every\ vertex\ in\ set\ 2$

$\boldsymbol{Subgraph}: A\ graph\ H\ is\ said\ to\ be\ subgraph\ iff\ every\ vertex\ in\ H\ is\ in\ G, every\ edge\ in\ H\ is\ in\ G\ and$

$each\ edge\ in\ H\ has\ the\ same\ endpoint\ as\ the\ same\ edge\ in\ G.$

$\boldsymbol{Connected\ Graph}$: $A\ graph\ is\ connected\ iff\ given\ any\ two\ vertices\ v\ and\ w\ in\ G, there\ will\ be\ a\ walk\ from\ v\ to\ w\ along\ the\ edges\ in\ G. i.e. \forall v, w \in V(G)\ \exists\ a\ walk\ P\ from\ v\ to\ w$

Degree:

$The\ degree\ of\ a\ vertex\ is\ the\ number\ of\ edges\ incident\ on\ that\ vertex\ in\ the\ graph\ G. Note\ that\ self-loops\ are\ counted\ twice. The\ total\ degree\ of\ the\ graph\ is\ the\ sum\ of\ all\ the\ degrees\ of\ each\ vertex\ in\ G$

Trails, Walks, Paths, Circuits, Closed walks, closed circuits, Simple circuits:

$Let\ G\ be\ a\ graph\ and\ let\ v\ and\ w\ be\ any\ two\ vertices\ in\ G.$

$\boldsymbol{Walk}$: $A\ finite\ alternating\ sequence\ of\ adjacent\ vertices\ and\ edges\ of\ g\ from\ v\ to\ w.$

$A\ walk\ is\ usually\ written\ as\ v_0 e_0 v_1 e_2 \ldots v_k. A\ walk\ to\ itself (one\ vertex\ only)\ is\ considered\ trivial.$

$\boldsymbol{Trail}$: $A\ walk\ from\ v\ to\ w\ without\ repeating\ edges$

$\boldsymbol{Path}$: $A\ walk\ from\ v\ to\ w\ without\ repating\ edges\ or\ vertexes$

$\boldsymbol{Closed\ Walk}$: $A\ walk\ from\ vertex\ v\ to\ itself$

$\boldsymbol{Circuit}$: $A\ closed\ walk\ that\ does\ have\ repeated\ edges$

$\boldsymbol{Simple\ Circuit}$: $A\ circuit\ that\ is\ path\ with\ only\ the\ endpoints\ being\ repeated$

$\boldsymbol{Connected}$: $Two\ vertices\ v\ and\ w\ are\ connected\ iff\ there\ is\ a\ walk\ from\ v\ to\ w$

$\boldsymbol{Connected\ component}$: $A\ graph\ H\ is\ called\ a\ a\ connected\ component\ of\ G\ iff$

$1. H\ is\ a\ subgraph\ of\ G, 2. H\ is\ connected, 3. No\ larger\ subgraph\ has\ edges\ or\ vertices\ that\ are\ not\ in\ H$

$\boldsymbol{Euler\ circuit}$: $A\ circuit\ in\ G\ that\ contains\ every\ vertex\ and\ edge\ in\ G\ . Vertices\ can\ be\ repeated.$

$\boldsymbol{Euler\ trail}$: $A\ trail\ in\ G\ that\ contains\ every\ vertex\ and\ edge\ in\ G. Vertices\ can\ be\ repeated.$

$\boldsymbol{Hamiltonian\ circuit}$: $A\ \ simple\ circuit\ containing\ every\ vertex\ in\ G.$

Isomorphic Graph:

$Two\ graphs\ G\ and\ G' are\ isomorphic\ to\ itself\ iff\ there\ exists\ a\ one\text{-}to\text{-}one\ correspondence\ between\ V(G) \rightarrow V(G') and\ E(G) \rightarrow E(G')\ that\ preserve\ edge\ endpoint\ functions. preserve\ of\ both\ graphs\ for\ all\ v \in V(G), V(G')\ and\ e \in E(G), E(G').$

Trees:

$A\ graph\ is\ a\ tree\ iff\ it\ is\ connected\ and\ is\ circuit\ free. If\ it\ is\ not\ connected\ it\ is\ called\ a\ forest$

$A\ tree\ with\ one\ vertex\ is\ a\ trivial\ tree.$

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*

Theorems:

Theorem 4.1.1:

$\forall a, b, c \in \mathbb{Z},\ if\ a|b\ and\ a|c, then\ \forall x, y \in \mathbb{Z}, a|(bx + cy)$

Proposition 4.2.2:

$For\ any\ two\ primes\ p\ and\ p'\ if\ p|p'\ then\ p = p'$

Theorem 4.2.3:

$If\ p\ is\ a\ prime\ and\ x_1, x_2, \ldots, x_n\ are\ any\ integers\ such\ that\ \ p \mid x_1 x_2 \ldots x_n,\ then\ p|x_i\ for\ some\ i \in [1, n]$

Theorem 4.3.1 (Epp):

$\forall a, b \in \mathbb{Z}^+, if\ a|b\ then\ a \leq b$

Theorem 4.3.3 (Epp):

$\forall a, b, c \in \mathbb{Z}, if\ a|b\ and\ b|c, then\ a|c$

Theorem 4.3.4 (Epp):

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

Theorem 4.3.5 (Epp):

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

$$n = p_1^{e_1} \times p_2^{e_2} \times \ldots \times p_k^{e_k}$$

$and\ any\ other\ expression\ for\ n\ as\ a\ product\ of\ its\ prime\ factors\ will\ be\ identical$

Proposition 4.7.3 (Epp):

$For\ any\ a \in \mathbb{Z}\ and\ any\ prime\ p, if\ p|a\ then\ p \nmid (a + 1)$

Theorem 4.7.4 (Epp):

$The\ set\ of\ primes\ is\ infinite$

Theorem 4.3.2 (Well Ordering Principle):

$If\ a\ nonempty\ subset\ S \subseteq \mathbb{Z}\ has\ a\ lower\ bound\ then\ S\ has\ a\ least\ element\ (minimum).$
$Similarly\ if\ the\ same\ subset\ S\ has\ an\ upper\ bound\ then\ S\ has\ a\ most\ element (maximum)$

Proposition 4.3.3:

$If\ a\ set\ S\ has\ a\ least\ element, its\ least\ element\ is\ unique$

Theorem 4.4.1 (Quotient Remainder Theorem):
$Given\ any\ integer\ a\ and\ any\ positive\ integer\ b, there\ exists\ unique\ integers\ q\ and\ r\ such\ that$

$$a = bq + r, 0 \leq r < b$$

Theorem 4.5.2(Bezout's Identity):

$Let\ a\ and\ b\ be\ integers\ where\ at\ ost\ one\ among\ a\ and\ b\ can\ be\ zero. Let\ d = \gcd(a,b).$

$Then\ there\ exists\ x,y \in \mathbb{Z}\ such\ that\ ax + by = d. Note\ that\ this\ identity\ is\ non-\ unique.$

Proposition 4.5.4

$For\ any\ integers\ a,b\ both\ nonzero\ if\ c|a\ and\ c|b\ then\ c|\gcd(a,b)$

Theorem 8.4.1 (Epp) (Modular Equivalences)

$Let\ a,b\ and\ n\ be\ integers\ where\ n > 1. The\ following\ statements\ are\ equivalent:$

$1. n|(a-b)$

$2. a \equiv b (mod\ n)$

$3. a = b + kn\ for\ some\ k \in \mathbb{Z}$

$4. a\ and\ b\ have\ the\ same\ remainder\ when\ divided\ by\ n$

$5. a(mod\ n) = b(mod\ n)$

Theorem 8.4.3 (Epp):

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

$1. a \equiv c\ (mod\ n)\ and\ 2. b \equiv d (mod\ n).$

$Then\ the\ following\ are\ equivalent:$

$1. (a \pm b) \equiv (c \pm d)\ (mod\ n)$

$2. ab \equiv cd\ (mod\ n)$

$3. a^m \equiv c^m (mod\ n), for\ positive\ integers\ m$

Corollary 8.4.4 (Epp):

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

$ab \equiv [(a\ mod\ n)(b\ mod\ n)](mod\ n)\ (i.e.\ ab\ mod\ n = (a\ mod\ n)(b\ mod\ n)\ mod\ n$

$Consequently, a^m \equiv [(a\ mod\ n)^m]\ (mod\ n)$

Theorem 4.7.3 (Existence of Multiplicative Inverse)

$For\ any\ integer\ a, its\ multiplicative\ inverse\ modulo\ n\ (where\ n > 1), a^{-1}, exists\ if\ and\ only$

$if\ \ a\ and\ n\ are\ coprime$

Corollary 4.7.4 (Special case: n is prime):

$If\ n = p\ is\ a\ prime\ number, then\ all\ integers\ in\ the\ range\ 0 < a < p\ have\ multiplicative$

$inverses\ modulo\ p.$

Theorem 8.4.9 (Epp)

$For\ all\ \ integers\ a,b,c,n\ \ with\ n > 1\ and\ a\ and\ n\ are\ coprime,$

$if\ ab \equiv ac\ (mod\ n), then\ b \equiv c\ (mod\ n)$

Theorem 5.1.1 (Epp)

$For\ any\ sequences\ of\ real\ numbers\ a_m, a_{m+1} \dots a_n\ and\ b_m, b_{m+1}, \dots b_n, the\ following\ equations\ are\ valid$

$for\ any\ , m \leq n\ and\ c \in \mathbb{R}$

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

$$2. c\left(\sum_{k=m}^{n} a_k\right) = \sum_{k=m}^{n} (c \cdot a_k)$$

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

Theorem 5.8.3(Epp) Distinct Roots Theorem:

$Suppose\ a\ sequence\ a_0, a_1, a_2 \dots satisfies\ the\ SLHRCC. If\ the\ characteristic\ eqn\ of$

$t^2 - At - B\ has\ two\ distinct\ roots, then\ the\ explicit\ formula\ for\ a_n\ can\ be\ denoted\ as:$

$$a_n = Cr^n + Ds^n, \qquad \forall n \in \mathbb{Z}$$

$where\ r\ and\ s\ are\ the\ roots\ of\ the\ characteristic\ equation\ and\ C\ and\ D$
$are\ constants\ determined\ by\ the\ initial\ conditions\ a_0\ and\ a_1$

Theorem 5.8.5(Epp)

$Suppose\ a\ sequence\ a_0, a_1, a_2 \dots satisfies\ the\ SLHRCC. If\ the\ characteristic\ eqn\ of$

$t^2 - At - B\ has\ only\ one\ real\ root, then\ the\ explicit\ formula\ for\ a_n\ can\ be\ denoted\ as:$

$$a_n = Cr^n + Dnr^n, \forall n \in \mathbb{Z}$$

$where\ r\ is\ the\ real\ root\ of\ the\ characteristic\ equation\ and\ C\ and\ D$
$are\ constants\ determined\ by\ the\ initial\ conditions\ a_0\ and\ a_1$

Theorem 6.2.1 (Epp):

$For\ all\ sets\ A, B\ and\ C$

$1. A \cap B \subseteq A\ and\ A \cap B \subseteq B, 2. A \subseteq A \cup B\ and\ B \subseteq A \cup B, 3. A \subseteq B\ and\ B \subseteq C, then\ A \subseteq C$

Theorem 6.2.2 (Epp):

$For\ all\ sets, A\ , B\ and\ C:$

$Same\ as\ tables\ regarding\ logical\ equivalences\ (\cup by\ OR\ and \cap\ by\ AND, 1 \equiv U\ and\ \phi \equiv 0).$

$With\ the\ addition\ of\ set\ difference\ where\ A - B = A \cap B^c$

Theorem 6.2.3 (Epp):

$Under\ proposition\ 6.4.4\ and\ 6.4.2$

Theorem 6.2.4 (Epp):

$The\ empty\ set\ is\ the\ subset\ of\ all\ sets$

Proposition 6.3.3 & Corollary 6.2.5(Epp):

$For\ any\ two\ sets\ X\ and\ Y, X \subseteq Y \wedge Y \subseteq X\ iff\ X = Y. Corollary: The\ empty\ set\ is\ unique.$

Proposition 6.4.2:

$Let\ A, B\ and\ C\ be\ sets,$ then

$$\bigcup \phi = \bigcup_{A \in \phi} \rightarrow A = \phi\ and \bigcup \{A\} = A$$

$A \cup \phi = A, A \cup B = B \cup A, (A \cup B) \cup C = A \cup (B \cup C), A \cup A = A\ and\ A \subseteq B \leftrightarrow A \cup B = B$

Proposition 6.4.4:

$Let\ A, B\ and\ C\ be\ sets,$ then

$A \cap \phi = \phi, A \cap B = B \cap A, A \cap (B \cap C) = (A \cap B) \cap C, A \subseteq B \leftrightarrow A \cap B = A$

$Distributivity\ laws: A \cap (B \cup C) = (A \cap B) \cup (A \cap C), A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Proposition 8.2.9 and 8.2.10:

8.2.9. $Composition\ is\ associative.$ 8.2.10 $And\ its\ inverse\ is\ such\ that: (\mathcal{R} \circ \mathcal{R}')^{-1} = \mathcal{R}'^{-1} \circ \mathcal{R}^{-1}$

Theorem 8.3.1

$Any\ partition\ of\ a\ set\ can\ be\ represented\ by\ an\ equivalence\ relation\ whose\ equivalence\ classes\ make$

$up\ the\ sets\ in\ the\ partition.$

Lemma 8.3.2 &8.3.3 (Epp):

$Given\ an\ equivalence\ relation\ \mathcal{R}\ on\ A, and\ where\ a, b \in A, a\ \mathcal{R}\ b \rightarrow [a] = [b].$ (8.3.2)

$Similarly\ if\ a \not\mathcal{R}\ b \rightarrow [a] \cap [b] = \phi. So\ [a] = [b]\ or\ [a] \cap [b] = \phi$ (8.3.3)

Theorem 8.3.4 (Epp):

$Any\ equivalence\ relation\ \mathcal{R}\ on\ set\ A\ will\ form\ a\ partition\ of\ set\ A\ by\ its\ distinct\ equivalence\ classes$

Proposition 8.5.2:

$The\ transitive\ closure\ of\ a\ relation\ \mathcal{R}\ can\ be\ obtianed\ by\ the\ union\ of\ repeated\ compositions\ of\ \mathcal{R}$

$$i.e\ \mathcal{R}^t = \bigcup_{i=1}^{\infty} \mathcal{R}^i$$

Proposition 7.2.4 (Existence of f^{-1})

$Let\ f\ be\ a\ function\ from\ S\ to\ T. Then\ f^{-1}\ is\ the\ inverse\ \boldsymbol{relation}\ from\ T\ to\ S. f^{-1}\ is\ a\ fucntion\ iff$

$f\ is\ bijective.$

Proposition 7.3.1 (Composition):

$Let\ f\ be\ a\ function\ from\ S\ to\ T, and\ g\ be\ a\ fucntion\ from\ T\ to\ U. Then\ the\ compostion\ of$

$g \circ f\ from\ S\ to\ U\ and\ f \circ g\ from\ U\ to\ S\ are\ also\ functions.$

Proposition 7.3.3

$Let\ f{:}\,A \rightarrow A\ be\ an\ injective\ function. Then\ f \circ f^{-1}\ is\ the\ identity\ function.$

$(f^{-1} \circ f = identity\ also\ \ if\ f\ is\ bijective)$

Theorem 9.1.1:

$If\ m\ and\ n\ are\ integers\ \ and\ m \leq n, then\ there\ are\ x =\ n - m + 1\ \ integers\ from\ m\ to\ n$

$inclusive\ of\ m\ and\ n.$

Theorem 9.2.1 (The Multiplication Rule):

$If\ an\ operation\ consists\ of\ k\ steps\ and\ each\ step\ i\ can\ be\ perfomed\ in\ n_i\ number\ of\ ways, independent$

$of\ the\ number\ of\ steps\ preceding\ step\ i\ the\ total\ number\ of\ the\ ways\ to\ complete\ the\ operation\ will\ be$

$$Number\ of\ ways = \prod_{i=1}^{k} n_i$$

Theorem 9.2.2 (Permutations of n objects):

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

Theorem 9.2.3 r-Permutations from a set of n elements

$The\ number\ of\ r - permutations\ from\ a\ set\ of\ n\ elements\ is\ given\ by\ the\ formula$

$P(n,r) = \dfrac{n!}{(n-r)!}\ where\ 1 \leq r \leq n$

Theorem 9.3.1 The Addition Rule

$Suppose\ a\ finite\ set\ A\ is\ equivalent\ tot\ he\ union\ of\ k\ distinct\ mutually\ disjoint\ subsets\ A_1, A_2, \ldots A_k.$

$Then, N(A) = N(A_1) + N(A_2) + \cdots N(A_k)$

Theorem 9.3.2 The Difference Rule

$The\ A\ is\ a\ finite\ set\ and\ B\ is\ a\ subset\ of\ A, then\ N(A - B) = N(A) - N(B)$

Theorem 9.3.3 The Inclusion-Exclusion Principle

$If\ A, B\ and\ C\ are\ finite\ sets\ , then\ the\ following\ hold\ true:$

$N(A \cup B) = N(A) + N(B) - N(A \cap B), and$

$N(A \cup B \cup C) = N(A) + N(B) + N(C) - N(A \cap B) - N(A \cap C) - N(B \cap C) + N(A \cap B \cap C)$

Generalized Pigeonhole Principle (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 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.

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.

Theorem 9.4.2

$If\ f\ is\ a\ function\ from\ X\ to\ Y, where\ X\ and\ Y\ are\ finite, f\ is\ on\ one\text{-}to\text{-}one\ iff\ f\ is\ onto$

Theorem 9.5.1

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

Theorem 9.5.2

$The\ number\ of\ ways\ to\ permute\ a\ collection\ of\ n\ objects\ with\ n\ distinguishable\ sets$

$is\ \dfrac{n!}{n_1!\,n_2!\,n_3!\,n_4!..n_k!}$

Theorem 9.6.1

$The\ number\ of\ r - combinations\ with\ repetition\ that\ can\ be\ selected\ from\ n\ elements\ is$

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

Pascal’s Formula(Theorem 9.7.1):

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

Binomial Theorem (Theorem 9.7.2):

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

Probability Axioms:

1. $0 \le P(A) \le 1,$
2. $P(\phi) = 0,$
3. $If\ A\ and\ B\ are\ disjoint\ (A \cap B = \phi), then\ P(A \cup B) = P(A) + P(B)$

Theorem 9.9.1-9.9.3:

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

9.9.2 $P(A \cap B) = P(B|A).P(A)$

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

Bayes’ Theorem:

$Suppose\ S\ is\ a\ sample\ space\ with\ n\ disjoint\ events\ B_1 - B_n.\ Suppose\ A\ is\ an\ event\ in\ S$

$and\ assume\ P(A), P(B_i) \neq 0\ where\ 0 \le i \le n. Then\ for\ any\ particular\ i$:

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

Theorem 10.1.1 (Handshake Theorem):

$A\ graph\ G\ with\ n\ edges\ has\ a\ total\ degree\ of\ 2n.i.e.\sum_{i=1}^{n}\deg(v_i) = 2n, where\ v_i \in G$

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

Corollary 10.1.2:

$The\ total\ degree\ of\ a\ graph\ is\ always\ even$

Propostition 10.1.3:

$In\ any\ graph\ there\ are\ an\ even\ number\ of\ vertices\ of\ an\ odd\ degree.$

Lemma 10.2.1:

$Let\ G\ be\ a\ graph.$

$(a) If\ G\ is\ connected\ then\ there\ is\ a\ path\ between\ any\ two\ vertices$

$(b) If\ v\ and\ w\ vertices\ are\ part\ of\ a\ circuit\ in\ G, and\ one\ edge\ is\ removed, there\ exists\ a\ trail\ between\ v\ and\ w$

$(c) If\ G\ is\ connected\ and\ G\ contains\ a\ circuit, then\ an\ edge\ of\ the\ circuit\ can\ be\ removed\ without\ disconnecting\ G$

Theorem 10.2.2:

$If\ a\ graph\ has\ an\ Euler\ circuit, every\ vertex\ in\ the\ graph\ has\ an\ even\ degree. If\ there\ exists\ any\ vertex\ with\ an\ odd\ degree, no\ Euler\ cirucit\ exits\ in\ that\ graph$

Theorem 10.2.3:

$Given\ a\ graph\ G\ is\ connected\ and\ all\ vertices\ have\ a\ positive\ even\ degree, then\ it\ has\ an\ Euler\ circuit.$

Theorem 10.2.4:

$Graph\ G\ has\ an\ Euler\ circuit\ \ iff\ G\ is\ connected\ and\ every\ vertex\ in\ G\ has\ an\ even\ degree$

Corollary 10.2.5:

$Let\ G\ be\ a\ graph, and\ let\ v\ and\ w\ be\ two\ distinct\ vertices\ of\ G. Then\ there\ is\ an\ euler\ trail\ from\ v\ to\ w\ if\ v\ and\ w\ have\ odd\ degrees\ and\ the\ rest\ of\ the\ vertices\ in\ G\ have\ a\ positive\ even\ degree$

Proposition 10.2.6

$If\ a\ graph\ G\ has\ a\ Hamiltonian\ circuit, then\ G\ has\ subgraph\ H\ with\ the\ following\ properties:$
$1. H\ contains\ every\ vertex\ of\ G, 2. H\ is\ connected, 3. H\ has\ has\ the\ same\ number\ of\ edges\ as\ vertices, 4. Every\ vertex\ of\ H\ has\ degree\ 2$

Adjacency Matrices:

$If\ a\ vertex\ i\ is\ adjacent\ to\ vertex\ j\ and\ there\ are\ k\ edges\ from\ i\ to\ j, then\ m_{ij} = k. Also,$

$in\ an\ undirected\ grpah, its\ adjacency\ matrix\ is\ always\ symmetric. An\ adjacency\ matrix\ A$
$of\ a\ graph\ G\ displays\ the\ walks\ from\ i\ to\ j\ of\ length\ 1\ at\ the\ entry\ \ m_{ij}. Subsequent\ powers\ of\ n$
$will\ give\ the\ walks\ of\ length\ n\ from\ i\ to\ j\ at\ the\ i, j^{th}\ entry$. (Theorem 10.3.2)

Theorem 10.4.1 (Isomorphism)

$If\ S\ is\ a\ set\ of\ grpahs\ and\ R\ be\ the\ relation\ of\ grpah\ isomorphism\ on\ S. Then\ R\ is\ an\ equivalence$
$relation\ on\ S$

Theorem 10.4.2 Graph Isomorphism invariants:

$If\ two\ graphs\ G\ and\ G'\ are\ isomorphic\ then\ the\ following\ hold\ true$:

1. $Both\ have\ n\ vertices$
2. $Both\ have\ m\ edges$
3. $Both\ have\ vertex\ of\ degree\ k, if\ exists\ in\ G$
4. $Both\ have\ m\ vertices\ of\ degree\ k\ if\ exists\ in\ G$
5. $Both\ have\ a\ circuit\ of\ length\ k, if\ exists\ in\ G$
6. $If\ G\ has\ a\ simple\ cirucit\ of\ length\ k, G'has\ it\ too$
7. $Has\ m\ simple\ circuits\ of\ length\ k, if\ exists\ in\ G$
8. $If\ G\ is\ connected, so\ is\ G'$
9. $If\ G\ has\ an\ Euler\ circuit, so\ does\ G'$
10. $If\ G\ has\ a\ Hamiltonian\ circuit, so\ does\ G'$

Lemma 10.5.1:

$Any\ nontrivial\ tree\ has\ at\ least\ one\ vertex\ of\ degree\ one$

Theorem 10.5.2:

$Any\ nontrivial\ tree\ with\ n\ vertices\ has\ n-1\ edges$

Lemma 10.5.3:

$If\ G\ is\ a\ connected\ graph\ , C\ is\ any\ circuit\ in\ G\ , and\ one\ of\ the\ edges\ of\ C\ is\ removed\ from\ G,$
$then\ the\ graph\ remains\ connected$

Theorem 10.5.4:

$A\ graph\ with\ n\ vertices\ and\ n-1\ edges\ is\ a\ tree$

Theorem 10.6.1: Full Binary Tree

$If\ T\ is\ a\ full\ binary\ tree\ with\ k\ internal\ vertices\ , then\ T\ has\ a\ total\ of\ 2k+1\ vertices$
$and\ has\ k+1\ terminal\ vertices$

Theorem 10.6.2

$For\ non-negative\ integers\ h, if\ T\ is\ a\ binary\ tree\ with\ height\ h\ and\ t\ terminal\ vertices,$

$then\ t \leq 2^h, i.e. \log_2 t \leq h$

Proposition 10.7.1

$Every\ connected\ graph\ has\ a\ spanning\ tree. Any\ two\ spanning\ trees\ have\ the\ same\ number\ of\ edges.$

$A\ spanning\ tree\ for\ a\ graph\ G\ is\ a\ subgraph\ which\ is\ a\ tree\ and\ contains\ every\ vertex\ in\ G$

F1. *Commutative Laws* For all real numbers *a* and *b*,
a + *b* = *b* + *a* and *ab* = *ba.*
F2. *Associative Laws* For all real numbers *a, b,* and *c,*
(a + b) + c = a + (b + c) and *(ab)c = a(bc).*
F3. *Distributive Laws* For all real numbers *a, b,* and *c,*
a(b + c) = ab + ac and *(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* and 1 · *a* = *a* · 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* = 0*,* there is a real number, denoted 1*/a* or *a*−1*,* called the **reciprocal** of *a,* such that
$a \cdot \frac{1}{a} = \frac{1}{a} \cdot a = 1$

A - 2 Appendix A Properties of the Real Numbers
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· *a* = *a* · 0 = 0.
T7. *Cancellation Law for Multiplication* If *ab* = *ac* and *a* = 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* = 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* ≠0, then *b/a* = *b*· *a*−1.
T10. If *a* ≠ 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), (−a)(−b) = ab,
and
$-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}$
T13. *Equivalent Fractions Property*

$$\frac{a}{b} = \frac{ac}{bc}\ if\ b \neq 0\ and\ c \neq 0$$

T14. *Rule for Addition of Fractions*
$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}\ b \neq 0\ and\ d \neq 0\ b$

T15. *Rule for Multiplication of Fractions*
$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}\ b \neq 0\ and\ d \neq 0$

T16. *Rule for Division of Fractions*

$$\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{ad}{bc} \ b \neq 0 \ and \ c \neq 0 \ and \ d \neq 0$$

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–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.

Given real numbers a and b,
$a < b$ means $b + (-a)$ is positive. $b > a$ means $a < b$.
$a \leq b$ means $a < b$ or $a = b$. $b \geq a$ means $a \leq b$.
If $a < 0$, we say that a is **negative.** If $a \geq 0$, we say that a is **nonnegative.**
From the order axioms Ord1–Ord3 and the above definition, all the usual rules for calculating with inequalities can be derived. The most important are collected as theorems
T17–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 $0 < ab < cd$