Sets	ℕ: {0,1,2,3,...}. ℤ: {...,-1,0,1,...}. ℚ: {1/2,-23,9.6} ℝ: real nums. ℂ: complex nums	0 neither negative nor positive. 0 is even ⇔: iff
Mathematical Statements	Statement/proposition is true or false but not both Universal conditional statement (universal + conditional): can be rewritten to make them purely universal/conditional Universal existential statement, existential universal statement, or any other combination	
Basic properties of Integers	∀x,y,z ∈ ℤ: Closure under addition & multiplication: x+y ∈ ℤ & xy ∈ ℤ Commutativity: x + y = y + x and xy = yx Associativity: x+y+z = (x+y)+z = x+(y+z) & xyz = (xy)z = x(yz) Distributivity: x(y+z) = xy + xz and (y+z)x = yx + zx Trichotomy: x=y or x<y or x>y (only 1 can be true)	n is even ⇔ ∃ an integer k s.t. n = 2k n is odd ⇔ ∃ an integer k s.t. n = 2k + 1 d is divisor/factor of n (d|n) ⇔ ∃ k ∈ ℤ s.t. n = dk (only for CS1231S) n is colorful if ∃ k ∈ ℤ s.t. n = 3k
	n is prime: (n>1) ∧ ∀r, s ∈ $\mathbb{Z}^+$, (n=rs → (r=1 ∧ s=n) ∨ (r=n ∧ s=1)	n is composite: ∃r,s ∈ $\mathbb{Z}^+$ (n=rs ∧ (1<r<n) ∧ (1<s<n))
Rational nums	r is rational ⇔ ∃ a,b ∈ ℤ s.t. r = a/b and b≠0	a/b is in lowest terms if the largest int that divides both a and b is 1

Proofs	Axiom/Postulate: statement assumed to be true w/o proof Corollary: simple deduction from theorem Conjecture: statement believed to be true; has no proof	Theorem: statement proved using rigorous mathematical reasoning (major result) Lemma: small theorem (minor result; purpose to help in proving theorem)	
	Direct proof	1. Let a and b be 2 consecutive odd nums ... 2. Product of 2 consecutive odd nums is always odd	
	Disproof by counterexample	Proof by mathematical induction	Combinatorial proof
	Proof by exhaustion	(suitable when num of cases if small) ∃ irrational nums p and q s.t. p^q is rational	
	Proof by deduction (type of direct proof; when num of cases is infinite)	1. Let nums be n and n+1 1.1 $(n+1)^2-n^2 = n^2+2n+1-n^2 = 2n+1$ (By algebra) 1.2 2n+1 is odd (by defn of odd nums) 2. Diff of any 2 consecutives squares is odd	
	Proof by contradiction	1. Suppose not, i.e.... Contradiction 2. Assumption is false, i.e....	
	Proof by contraposition	Proof ~q → ~p. Conclude p → q	

Theorem 4.2.1	Every integer is a rational number		
Theorem 4.2.2	Sum of any two rational nums is rational		
Corollary 4.2.3	Double of a rational number is rational		
Theorem 4.3.1	For all positive integers a and b, if a|b, then a ≤ b		
Theorem 4.3.2	The only divisors of 1 are 1 and -1		
Theorem 4.3.3	Transitivity of Divisibility: For all integers a,b and c, if a|b and b|c, then a|c		
Theorem 4.4.1	Quotient-Remainder Theorem: Given any int n and positive int d, ∃ unique ints q and r s.t. n = dq + r and 0 ≤ r < d		
Lemma 4.4.4	For any r ∈ ℝ, =|r| ≤ r ≤ |r|		
Theorem 4.4.6	Triangle Inequality: For any x, y ∈ ℝ, |x+y| ≤ |x|+|y|		
Theorem 4.6.1	There is no greatest integer		
Proposition 4.6.4	∀ integers n, if n^2 is even, then n is even		
Theorem 4.7.1	√2 is irrational		
T1Q10	Let n be an ∈ ℤ. Then n^2 is odd iff n is odd	T2Q10	Let a, b ∈ $\mathbb{Z}^+$. If n = ab, then a ≤ $\sqrt{a}$ or b ≤ $\sqrt{b}$

Properties of real nums (Appendix A)

F1. Commutative Laws	∀ real nums a,b: a+b = b+a and ab = ba	F2. Associative Laws	∀ real nums a,b,c: (a+b)+c = a+(b+c) and (ab)c = a(bc)
F3. Distributive Laws	∀ real nums a,b,c: a(b+c) = ab+ac and (b+c)a = ba + ca	F4. Existence of Identity Elements	∃ 2 distinct real nums, 0 and 1, s.t. for every real num a: 0+a = a+0 = a and 1*a = a*1 = a
F5. Existence of Additive Inverses	For every real num a, ∃ a real num -a of a, s.t. a + (-a) = (-a) + a = 0	F6. Existence of Reciprocals	For every real num a ≠ 0, ∃ a real num 1/a or a^{-1} s.t. a*(1/a) = (1/a)*a = 1
T1. Cancellation Law for Addition	If a+b = a+c, then b = c	T2. Possibility of Subtraction	Given a and b, there is exactly one x s.t. a+x = b. This x = b-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	T8. Possibility of Division	Given a and b w a ≠ 0, there is exactly one x s.t. ax = b. This x = b/a and is the quotient of b and a
T9.	If a ≠ 0, then $b/a = ba^{-1}$	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 w Negative Signs	(-a)b = a(-c) = -(ab), (-a)(-b) = ab, $-\frac{a}{b}=\frac{-a}{b}=\frac{a}{-b}$
T13. Equivalent Fractions Property	$\frac{a}{b}=\frac{ac}{bc}$, if b ≠ 0 and c ≠ 0	T14. Rule for Addition of Fractions	$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$, if b ≠ 0 and c ≠ 0
T15. Rule for Multiplication of Fractions	$\frac{a}{b}*\frac{c}{d}=\frac{ac}{bd}$, if b ≠ 0 and d ≠ 0	T16. Rule for Division of Fractions	$\frac{\frac{a}{b}}{\frac{c}{d}}=\frac{ad}{bc}$, if b ≠ 0, c ≠ 0 and d ≠ 0
Positive real nums satisfy Ord1-3	Ord1. For any real nums a and b, if a and b are positive, so are a+b and ab	Ord2. For every real num a ≠ 0, either a is +ve or -a is +ve, but not both	Ord3. 0 is not positive
T17. Trichotomy Law	For any real nums a and b, exactly 1 of the 3 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 ≠ 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		

Compound Statements	~: not/negation (others use ¬) ∧: and/conjunction	∨: inclusive or/disjunction (A or B or both) unlike exclusive or (A or B but not both; XOR)	
Order of ops	~: performed first	∧, ∨ are coequal (use parentheses to disambiguate order of ops)	↔, → are coequal: performed last
Statement form	Expression made up of statement vars and logical connectives that becomes a statement when actual statements are sub for the component statements vars (e.g. 3+n=9,, 2x = x^2)		

Logical Equivalence	2 statements forms are logically equivalent iff they have identical truth values for each possible sub of statements for their statement vars. $P \equiv Q$ Prove not equivalent: 1) construct truth table OR 2) find counter example		Tautology: statement form that is always true Contradiction: statement form that is always false
Theorem 2.1.1	Commutative laws	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
	Associative laws	$p \wedge q \wedge r \equiv (p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$p \vee q \vee r \equiv (p \vee q) \vee r \equiv p \vee (q \vee r)$
	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	$p \wedge \text{true} \equiv p$	$p \vee \text{false} \equiv p$
	Negation laws	$p \vee {\sim}p \equiv \text{true}$	$p \wedge {\sim}p \equiv \text{false}$
	Double negative laws	${\sim}({\sim}p) \equiv p$	
	Idempotent laws	$p \wedge p \equiv p$	$p \vee p \equiv p$
	Universal bound laws	$p \vee \text{true} \equiv \text{true}$	$p \wedge \text{false} \equiv \text{false}$
	De Morgan's Laws	${\sim}(p \wedge q) \equiv {\sim}p \vee {\sim}q$	${\sim}(p \vee q) \equiv {\sim}p \wedge {\sim}q$ (not and not OR neither nor)
	Absorption laws	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
	Negation of true and false	${\sim}\text{true} \equiv \text{false}$	${\sim}\text{false} \equiv \text{true}$
Conditional Statements	If p then q OR p implies q OR q if p OR $p \to q$. It is false when p is true and q is false; otherwise it is true p is the hypothesis/antecedent of the conditional and q the conclusion/consequent Conditional statement is vacuously true/true by default (i.e. if p is false, statement as a whole is true by default)		
Implication Law	$p \to q \equiv {\sim}p \vee q$ (proof using truth table)		Negation of conditional statement: ${\sim}(p \to q) \equiv p \wedge {\sim}q$
Contrapositive, Converse & Inverse of a conditional statement	Contrapositive of $p \to q$ is ${\sim}q \to {\sim}p$ $p \to q \equiv {\sim}q \to {\sim}p$ (conditional statement $\equiv$ contrapositive) Note $p \to q \not\equiv q \to p \not\equiv {\sim}p \to {\sim}q$ (conditional $\not\equiv$ inverse or converse)		Converse of $p \to q$ is $q \to p$ Inverse of $p \to q$ is ${\sim}p \to {\sim}q$ $q \to p \equiv {\sim}p \to {\sim}q$ (converse $\equiv$ inverse)
Only If and Biconditional	p **only if** q means if not q then not p, ${\sim}q \to {\sim}p \equiv p \to q$		Biconditional of p and q is p **if and only if** (iff) q, $p \leftrightarrow q$ $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$ (true if both p,q have same truth values)
Necessary and Sufficient	r is a sufficient condition for s: if r then s OR $r \to s$ r is a necessary condtion for s: if not r then not s OR if s then r OR $s \to r$ (r alone might not imply s occur)		r is a necessary and sufficient condition for s: r iff s OR $r \leftrightarrow s$
Arguments	Argument form is valid iff whenever statements are substituted that make all the premises true, conclusion is also true Premises/assumptions/hypothesis: statements except final one Conclusion: final statement	Testing an argument form for validity: 1. Identify premises and conclusion of the argument form 2. Construct truth table of all the premises and conclusion 3. A row of the truth table in which all the premises are true aka critical row a) If $\exists$ critical row in which conclusion is false, $\Rightarrow$ argument form is invalid b) If conclusion in every critical row is true $\Rightarrow$ argument form is valid	
Modus Ponens & Modus Tollens	Syllogism: argument form consisting of 2 premises and conclusion (e.g. Modus Ponens or Modus Tollens; both are valid form of argument)		
Fallacies	Error in reasoning, resulting in invalid argument (e.g. using ambiguous premises and treating them as unambiguous, circular reasoning [assuming what is to be proved w/o deriving from premises], jumping to conclusion) Argument is sound iff it is valid, and all its premises are true (opp is unsound)		
	Converse error	$p \to q$, q, $\therefore$ p (aka fallacy of affirming the consequence)	
	Inverse error	$p \to q$, ${\sim}p$, $\therefore {\sim}q$	
	False premise	Argument is valid, but premise is false. E.g. If Singaporean, then must be 2m tall	
Contradiction Rule	If an assumption leads to a contradiction, then that assumption must be false (used in proof by contradiction)		

Table 2.3.1 Rules of Inference (Form of argument that is valid)

Modus Ponens	if p then q p $\therefore$ q	Modus Tollens	if p then q ${\sim}q$ $\therefore {\sim}p$	Proof by Division into Cases	$p \vee q$ $p \to r$ $q \to r$ $\therefore r$	Conjunction	p q $p \wedge q$
Elimination	$p \vee q$ OR $p \vee q$ ${\sim}q$ ${\sim}p$ $\therefore p$ $\therefore q$	Transitivity	$p \to q$ $q \to r$ $\therefore p \to r$	T1Q6d	$p \to r$ $q \to r$ $\therefore p \vee q \to r$		
Generalization	p OR q $\therefore p \vee q$ $\therefore p \vee q$	Specialization	$p \wedge q$ OR $p \wedge q$ $\therefore p$ $\therefore q$	Contradiction Rule	${\sim}p \to \text{false}$ $\therefore p$		

Truth table

p	q	~p	$p \wedge q$	$p \vee q$	$p \to q$	${\sim}q \to {\sim}p$ (contrapositive)	$q \to p$ (converse)	${\sim}p \to {\sim}q$ (inverse)	$p \leftrightarrow q$ (iff)
T	T	F	T	T	T	T	T	T	T
T	F	F	F	T	F	F	T	T	F
F	T	T	F	T	T	T	F	F	F
F	F	T	F	F	T	T	T	T	T

Predicate	Predicate: sentence that contains a finite num of vars and become a statement when specific values are sub for the vars Domain of a predicate var is the set of all values that may be substituted in place of the var 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, i.e. $\{x \in D \mid P(x)\}$, ($\mid$ mean s.t. in set theory)
Quantifier	Universal quantifier: $\forall$, for all Let Q(x) be a predicate and D the domain of x. A universal statement is a statement of the form $\forall x \in D, Q(x)$ Statement true iff Q(x) is true for every x in D & Statement false iff Q(x) is false for at least one x in D (counterexample)
	Existential quantifier: $\exists$, there exist. $\exists!$: there exists a unique 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) Statement true iff Q(x) is true for at least one x in D & Statement false iff Q(x) is false for all x in D
Universal Conditional Statement	$\forall x\, (P(x) \to Q(x))$
Equivalent Forms	Universal: By narrowing U to domain D consisting of all values of x that make P(x) true: $\forall x \in U\, (P(x) \to Q(x)) \Rightarrow \forall x \in D\, Q(x)$ Existential: $\exists x$ s.t. (P(x) and Q(x)) $\Rightarrow \exists x \in D$ s.t. Q(x), where D is the set of all x for which P(x) is true
	Factor: an integer that multiplied with another integer gives n, i.e. can be negative int Prime num: int whose positive integer factors are itself and 1
Implicit Quantification	Predicate If $x > 2$, then $x^2 > 4$ is implicit implying $\forall$real num x, (if $x > 2$ then $x^2 > 4$)

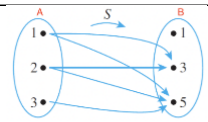
Negation of quantified statement	**Thrm 3.2.1:** Negation of universal statement: $\sim(\forall x\in D, P(x)) \equiv \exists x\in D$ s.t. $\sim P(x)$ **Thrm 3.2.2:** Negation of existential statement: $\sim(\exists x\in D \text{ s.t. } P(x)) \equiv \forall x\in D, \sim P(x)$ Negation of universal conditional statement: $\sim(\forall x\,(P(x) \to Q(x))) \equiv \exists x\in D$ s.t. $\sim(P(x) \to Q(x)) \equiv \exists x\in D$ s.t. $(P(x) \wedge \sim Q(x))$			
Relation	$\forall x\in D, P(x) \equiv P(x_1) \wedge P(x_2) \wedge \ldots \wedge P(x_n)$	$\exists x\in D$ s.t. $P(x) \equiv P(x_1) \vee P(x_2) \vee \ldots \vee P(x_n)$		
Vacuous Truth	$\forall x\,(P(x) \to Q(x))$ is vacuously true/true by default iff P(x) is false for every x in D, i.e. if its negation $\exists x\in D$ s.t. $(P(x) \wedge \sim Q(x))$ is false, then original statement is true by default Vacuous truth: true because the hypothesis (antecedent) cannot be satisfied			
Variants of Universal Conditional Statement	$\forall x\in D\,(P(x) \to Q(x))$, logically equivalent to contrapositive Contrapositive: $\forall x\in D\,(\sim Q(x) \to \sim P(x))$	Converse: $\forall x\in D\,(Q(x) \to P(x))$ Inverse: $\forall x\in D\,(\sim P(x) \to \sim Q(x))$		
Necessary, Sufficient Cond^n, Only if	$\forall x$ r(x) is a sufficient condition for s(x) means $\forall x\,(r(x) \to s(x))$ $\forall x$ r(x) is a necessary condition for s(x) means $\forall x\,(\sim r(x) \to \sim s(x)) \equiv \forall x\,(s(x) \to r(x))$ $\forall x$ r(x) only if s(x) means $\forall x\,(\sim s(x) \to \sim r(x)) \equiv \forall x\,(r(x) \to s(x))$			
Multiple Quantifiers	$\forall x\in D, \exists y\in E$ s.t. P(x,y): every elem x in D, there is a y in E that "works" for x $\exists x\in D$ s.t. $\forall y\in E$, P(x,y): 1 x in D that "works" no matter which y in E is chosen			
Negations of Multiple-Quantified Statements	$\sim(\forall x\in D, \exists y\in E \text{ s.t. } P(x,y)) \equiv \exists x\in D, \forall y\in E, \sim P(x,y)$ $\sim(\exists x\in D \text{ s.t. } \forall y\in E, P(x,y)) \equiv \forall x\in D, \exists y\in E$ s.t. $\sim P(x,y)$			
Order of quantifiers	In a statement containing both ∀ and ∈, changing order of quantifiers, changes meaning of statement. However, if both quantifiers are of same type, then order don't matter			
Formal Logical Notation	$\forall x\in D, P(x)$ as $\forall x\,(x\in D \to P(x))$ $\exists x\in D$ s.t. P(x) as $\exists x\,(x\in D \wedge P(x))$ For this module, follow 1st type of notation	2nd type usually used in AI, automata theory, formal languages Taken tgt, the symbols for quantifiers, vars, predicates and logical connectives is known as language of first-order logic		
Universal instantia-tion	If some property is true of everything in the set, then it is true of any particular thing in the set Fundamental tool of deductive reasoning	Universal Modus Ponens	$\forall x\,(P(x) \to Q(x))$ P(a) for a particular a ∴ Q(a)	
Universal Modus Tollens	$\forall x\,(P(x) \to Q(x))$ ~Q(a) for a particular a ∴ ~P(a) Used in proof of contradiction	Universal Transitivity	$\forall x\,(P(x) \to Q(x))$ $\forall x\,(Q(x) \to R(x))$ ∴ $\forall x\,(P(x) \to R(x))$	
Validity of args w Quantified statement	Same for args w compound statements Arg valid iff truth of its conclusion follows necessarily from truth of its premises. **Defn 3.4.1:** arg form is valid means 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 Arg is valid iff its form is valid. Can use venn diagrams to show validity/invalidity of args			
Converse, Inverse error	Converse error: $\forall x\,(P(x) \to Q(x))$ Q(a) for a particular a ∴ P(a)	Inverse error: $\forall x\,(P(x) \to Q(x))$ ~P(a) for a particular a ∴ ~Q(a)		
Rules of Inference for Quantified Statement	Universal instantiation	$\forall x\in D, P(x)$ ∴ P(a) if $a\in D$	Existential instantiation	$\exists x\in D, P(x)$ ∴ P(a) for some $a\in D$
	Universal generalization	P(a) for every $a\in D$ ∴ $\forall x\in D, P(x)$	Existential generalization	P(a) for some $a\in D$ ∴ $\exists x\in D, P(x)$

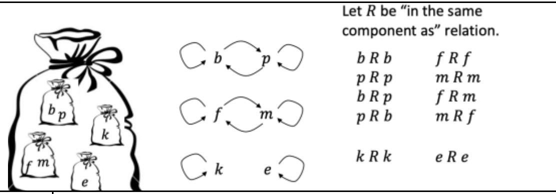
Set Theory	Set: unordered collection of objects Objects: members or elems of set - Order and duplicates do not matter If S is a set, $x \in S$ means x is an elem of S Cardinality of set S: $\|S\|$ is the size of the set, i.e. num of elems	Set Roster Notation: {1,2,3}, {1,2,3,...,100} Set-builder notation: Set of all elems $x \in U$ s.t. P(x) is true is denoted $\{x \in U{:}P(x)\}$ or $\{x \in U \mid P(x)\}$ Replacement notation: Set of all objs of the form t(x) where x ranges over elems of A is denoted $\{t(x){:}\ x \in A\}$ or $\{t(x) \mid x \in A\}$	
Subsets, Proper Subsets, Empty Set and Singleton	A is subset of B, i.e. $A \subseteq B$ iff every elem of A is also an elem of B or $A \subseteq B$ iff $\forall x\,(x \in A \to x \in B)$		
	A is a proper subset of B, $A \subsetneq B$ iff $A \subseteq B$ and $A \neq B$. $A \nsubseteq B \Leftrightarrow \exists x\,(x\in A \wedge x\notin B)$	Empty set: Set w no elem, {}, denoted as ∅ Singleton: set w exactly 1 elem	
Ordered Pairs	Ordered pair is an expression of the from (x,y)	$(a,b) = (c,d) \Leftrightarrow (a=c) \wedge (b=d)$	
Cartesian Products	Given sets A and B, Cartesian product of A and B, denoted A×B (read as A cross B), is set of all ordered pairs (a,b) where a is in A and b is in B $A\times B = \{(a,b){:}\ a\in A \wedge b\in B\}$	$\mathbb{R} \times \mathbb{R}$ is set of all ordered pairs (x,y) where $x, y \in \mathbb{R}$, i.e. Cartesian plane	
Set Equality	A = B iff every element of A is in B and every elem of B is in A	$A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$ OR $\forall x\,(x \in A \Leftrightarrow x \in B)$	
Venn Diagrams	Note $\{x\} \neq \{x, \emptyset\}$		
Operations on Sets	Universal set: e.g. certain mathematical situations all sets considered are sets of real nums Let A and B be subsets of a universal set U 1. $A \cup B$: set of all elements that are in at least 1 of A or B 2. $A \cap B$: set of all elems that are common to both A and B 3. B - A or B\A (diff of B minus A/relative complement of A in B): set of all elems in B and not in A 4. $\bar{A}$ (complement of A, A^C): set of all elems in U not in A	(Elements mtd) 1. $A \cup B = \{x\in U{:}\ x\in A \vee x\in B\}$ 2. $A \cap B = \{x\in U{:}\ x\in A \wedge x\in B\}$ 3. $B\backslash A = \{x\in U{:}\ x\notin A \wedge x\in B\}$ 4. $\bar{A} = \{x\in U{:}\ x\notin A\}$	
	$\bigcup_{i=0}^{n} A_i = A_0 \cup A_1 \cup \ldots \cup A_n$	$\bigcap_{i=0}^{n} A_i = A_0 \cap A_1 \cap \ldots \cap A_n$	
Partition of Sets	Sets can be divided into nonoverlapping (disjoint) pieces. Such a division is called a partition, e.g. $\{A_1, A_2, A_3\}$: partition of A 2 sets are disjoint iff they have no elems in common, i.e. A and B are disjoint iff $A \cap B = \emptyset$ Sets $A_1, A_2, \ldots$ are mutually disjoint (pairwise disjoint) iff no two sets A_i and A_j w distinct subscripts have any elems in common, i.e. for all i,j=1,2,..., i.e. $A_i \cap A_j = \emptyset$ whenever $i \neq j$		
Power Sets	Power set of A, P(A) is the set of all subsets of A	E.g. A = {x,y}. Then P(A) = {∅, {x}, {y}, {x,y}} If A has n elems, then its power set P(A) has 2^n elems	
Ordered n-tuples	Let $n \in \mathbb{Z}^+$ and let $x_1, x_2, \ldots, x_n$ be (not necessarily distinct) elems. Ordered n-tuple is of the form $(x_1,x_2,\ldots,x_n)$ Order pair is an ordered 2-tuple; ordered triple is an ordered 3-tuple Cartesian product of $A_1, A_2, \ldots, A_n$ denoted $A_1 \times A_2 \times \ldots \times A_n$ is set of all ordered n-tuples $(a_1,a_2,\ldots,a_n)$ where $a_i \in A_i$, i = 1,...,n i.e. $A_1 \times A_2 \times \ldots \times A_n = \{(a_1,a_2,\ldots,a_n){:}\ a_1 \in A_1 \wedge a_2 \in A_2 \wedge \ldots \wedge a_n \in A_n\}$ If A is a set, then $A^n = A\times A\times\ldots\times A$ (n times)		

Properties of Sets	1. Inclusion of Intersection: For all sets A and B, (a) $A \cap B \subseteq A$, (b) $A \cap B \subseteq B$ 2. Inclusion in Union: for all sets A and B, (a) $A \subseteq A \cup B$, (b) $B \subseteq A \cup B$ 3. Transitive property of Subsets: For all sets A,B and C, $A \subseteq B \wedge B \subseteq C \rightarrow A \subseteq C$	
Procedural Versions of Set Def^n	1. $a \in X \cup Y \Leftrightarrow (a \in X) \vee (a \in Y)$ 2. $a \in X \cap Y \Leftrightarrow (a \in X) \wedge (a \in Y)$ 3. $a \in X - Y \Leftrightarrow (a \in X) \wedge (a \notin Y)$	4. $a \in \bar{X} \Leftrightarrow a \notin X$ 5. $(a,b) \in X \times Y \Leftrightarrow (a \in X) \wedge (b \in Y)$
Theorem 6.2.1	1. Inclusion of Intersection: For all sets A and B, (a) $A \cap B \subseteq A$, (b) $A \cap B \subseteq B$ 2. Inclusion in Union: for all sets A and B, (a) $A \subseteq A \cup B$, (b) $B \subseteq A \cup B$ 3. Transitive property of Subsets: For all sets A,B and C, $A \subseteq B \wedge B \subseteq C \rightarrow A \subseteq C$	
Theorem 6.2.2 Set Identities	Let all set below be subsets of a universal set U	

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

Theorem 6.2.4	An empty set is a subset of every set, i.e. $\emptyset \subseteq A$ for all sets A
Theorem 6.3.1	Suppose A is a finite set w n elems, then P(A) has 2^n elems. i.e. $\|P(A)\| = 2^{\|A\|}$
T3Q8	$A \subseteq B$ iff $A \cup B = B$

Relations on Sets	Let A and B be sets. A (binary) relation from A to B is a subset of $A \times B$ Given an ordered pair(x,y) in $A \times B$, x is related to y by R, or x is R-related to y, written x R y, iff $(x,y) \in R$ x R y means $(x,y) \in R$. x [R with slash across] y means $(x,y) \notin R$	E.g. Let A = {0,1}, B = {1,2}. Define R s.t xRy iff x < y Then 0R1, 0R2, 1R2 R = {(0,1), (0,2), (1,2)}
	Let A and B be sets and R be a relation from A to B Domain of R, Dom(R) is the set{a∈A: aRb for some b∈B} Co-domain of R, coDom(R), is the set B Range of R, Range(R) is the set{b∈B: aRb for some a∈A}	Let A = {1,2,3}, B = {2,4,9}. Define relation R from A to B as: $\forall(x,y) \in A \times B, (x,y) \in R \Leftrightarrow x^2 = y$ Dom(R) = {2,3}, coDom(R) = {2,4,9} Range(R) = {4,9}
	R from A to B can also be depicted as an arrow diagram: - Represent elems of A as pts in 1 region and elems of B as pts in another region - For each $x \in A$ and $y \in B$, draw an arrow from x to y iff xRy E.g. Let A = {1,2,3}, B = {1,3,5}. Define relation S as: $\forall(x,y) \in A \times B, (x,y) \in S \Leftrightarrow x < y$	
Inverse of a Relation	Let R be a relation from A to B. Define the inverse relation R^{-1} from B to A as: $R^{-1} = \{(y,x) \in B \times A: (x,y) \in R\}$ OR $\forall x \in A, \forall y \in B\ ((y,x) \in R^{-1} \Leftrightarrow (x,y) \in R)$	
Directed Graph of a Relation	A relation on set A is a relation from A to A. (i.e. a subset of $A \times A$) $A \times A = A^2$. In general A^n is $A \times \ldots \times A$ (n times) Arrow diagram of such a relation can be modified so that it becomes a directed graph. - Represent A only once, instead of 2 separate sets of pts, and draw an arrow from each pt of A to its related pt. - If pt is related to itself, draw loop that extends out from the pt and goes back to it	
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 s.t. $\forall x \in A, \forall z \in C\ (x\ S \circ R\ z \Leftrightarrow (\exists y \in B\ (xRy \wedge ySz)))$ i.e. There is some "path" from x to z via some intermediate elem y in B in arrow diagram	
	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 a composition. Let A,B and C be sets. Let $R \subseteq A \times B$ and $S \subseteq B \times C$ be relations $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$	
N-ary Relations and Relational Databases	Given n sets $A_1, A_2, \ldots, A_n$, an n-ary relation R on $A_1 \times A_2 \times \ldots \times A_n$ is a subset of $A_1 \times A_2 \times \ldots \times A_n$. The special cases of 2-ary, 3-ary and 4-ary are called binary, ternary and quaternary relations	
Reflexivity, Symmetry & Transitivity	Let R be a relation on a set A 1. R is reflexive iff $\forall x \in A\ (xRx)$ (arrow to itself) 2. R is symmetric iff $\forall x,y \in A\ (xRy \Rightarrow yRx)$ (arrow both ways) 3. R is transitive iff $\forall x,y,z \in A\ (xRy \wedge yRz \Rightarrow xRz)$ (arrow from 1 to 2, 2 to 3 and 1 to 3) **T4Q2**: R is symmetric $\equiv \forall x,y \in A\ (xRy \Leftrightarrow yRx) \equiv R = R^{-1}$	Define relation R on $\mathbb{Z}$ as: $\forall x,y \in \mathbb{Z}\ (xRy \Leftrightarrow 3\|(x-y))$ aka congruence modulo 3 R is reflexive, symmetric & transitive
Asymmetry & Irreflexive	R is asymmetric iff $\forall x,y \in A\ (xRy \Rightarrow$ y NOT Rx, i.e. $(y,x) \notin R)$ Relation $\prec$ on A is irreflexive iff $\forall x \in A, (x \nprec x)$	Asymmetric $\Rightarrow$ Antisymmetric (vacuously true)
Strict Partial Order	A relation is a strict partial order iff it is irreflexive, antisymmetric and transitive	
Chain	Let $\prec$ be a strict partial order on a set A. A subset C of A is a chain iff each pair of distinct elements in C is comparable, i.e. $\forall a,b \in C\ (a \neq b) \Rightarrow (a \prec b \vee b \prec a)$ A maximal chain is a chain M s.t. $t \notin M \Rightarrow M \cup \{t\}$ is not a chain	
Transitive Closure of a Relation	Generally, a relation fails to be transitive as it fails to contain certain ordered pairs. E.g. (1,3), (3,4) in R, then (1,4) must also be in R Relation obtained by adding the least num of ordered pairs to ensure transitivity is called the transitive closure of the relation Transitive Closure: Let A be a set and R a relation on A. Transitive closure of R is the relation R^t on A that satisfies: 1) R^t is transitive. 2) $R \subseteq R^t$. 3) If S is any other transitive relation that contains R, then $R^t \subseteq S$	
Relation Induced by a Partition	A **partition** of a set A is a finite or infinite collection of nonempty, mutually disjoint subsets whose union is A $\mathcal{C}$ is a partition of a set A if (1) $\mathcal{C}$ is a set of which all elems are non-empty subsets of A, i.e. $\emptyset \neq S \subseteq A$ for all $S \in \mathcal{C}$ (2) Every elem of A is in exactly 1 elem of $\mathcal{C}$, i.e. $\forall x \in A\ \exists S \in \mathcal{C}\ (x \in S)$ & $\forall x \in A\ \forall S_1,S_2 \in \mathcal{C}\ (x \in S_1 \wedge x \in S_2 \Rightarrow S_1 = S_2)$ OR A partition of a set A is a set $\mathcal{C}$ of non-empty subsets of A s.t. $\forall x \in A\ \exists! S \in \mathcal{C}\ (x \in S)$ [$\exists!$: there exists a unique]	

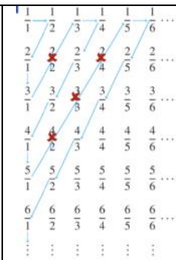
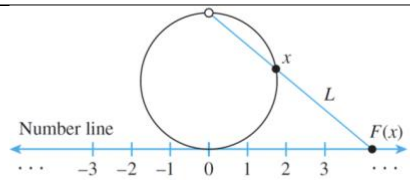
	Elems of a partition are called components of the partition	
Partitions as relations	We may view a partition as a "is in the same components as" relation Given a partition $\mathcal{C}$ of a set A, the relation R induced by the partition is: ∀x,y ∈ A, xRy ⇔ ∃a component S of $\mathcal{C}$ s.t. x,y∈S **Thrm 8.3.1** Let A be a set w a partition and let R be the relation induced by the partition. Then R is reflexive, symmetric, and transitive (vacuously true)	
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. (~ to denote equivalence relation)	Must prove all 3 properties to prove equivalence relation
Equivalence Classes of an Equivalence Relation	Suppose A is a set and ~ is an equivalence relation on A. For each a∈A, the equivalence class of a, denoted [a] (aka class of a), is the set of all elements x∈A s.t. a is ~-related to x $[a]_\sim$ = {x∈A: a~x}, OR ∀x ∈ A (x∈ $[a]_\sim$ ⇔ a~x)	
	E.g. Let A = {0,1,2,3,4} and define relation R on A as: R = {(0,0), (0,4), (1,1), (1,3), (2,2), (3,1), (3,3), (4,0), (4,4)} [0] = {0,4}, [1] = {1,3}, [2] = {2}, [3] = {1,3}, [4] = {0,4} Since [0] = [4] and [1] = [3]. The distinct equivalence class of the relation are {0,4}, {1,3} and {2}	
Lemma Rel.1 Equivalence Classes	Let ~ be an equivalence relation on a set A. The following are equivalent for all x,y ∈ A. (i) x~y. (ii) [x] = [y]. (iii) [x] ∩ [y] ≠ ∅	
Thrm 8.3.4	Partition Induced by an Equivalence Relation: If A is a set and R is an equivalence relation on A, then the distinct equivalence classes of R form a partition of A; i.e. union of the equivalence classes is all of A, and the intersection of any 2 distinct classes is empty	
Congruence	Divisibility: Let n, d ∈ $\mathbb{Z}$. Then $d\mid n$ ⇔ n = dk for some k ∈ $\mathbb{Z}$ Congruence: Let a,b ∈ $\mathbb{Z}$, n ∈ $\mathbb{Z}^+$. Then a is congruent to b modulo n iff a-b = nk for some k ∈ $\mathbb{Z}$. i.e. $n\mid$(a--b). a≡b (mod n)	
Proposition	Congruence-mod n is an equivalence relation on $\mathbb{Z}$ for every n ∈ $\mathbb{Z}^+$ Note [x] = [x+n] for equivalence classes of congruence-mod-n	
Dividing a Set by an Equivalence Relation	Let A be a set and ~ be an equivalence relation on A. Denote by A/~ the set of all equivalence classes w.r.t ~, i.e. A/~ = {$[x]_\sim$: x∈A} (A/~: quotient of A by ~)	
	Thrm Rel.2 Equivalence classes form a partition: Let ~ be an equivalence relation on a set A. Then A/~ is a partition of A	
Summary	A relation on set A is a subset of A^2 If R is a relation on a set A, then we write x R y for (x,y) ∈ R A partition of a set A is a set $\mathcal{C}$ of non-empty subsets of A s.t. ∀x ∈ A ∃!S ∈ $\mathcal{C}$ (x∈S) A relation R on A is an equivalence relation if 1. reflexive: ∀x ∈ A (xRx) 2. symmetric: ∀x,y ∈ A (xRy ⇒ yRx) 3. transitive: ∀x,y,z ∈ A (xRy ∧ yRz ⇒ xRz) Let ~ be an equivalence relation on A. Then the set of all equivalence classes is denoted by A/~ = {$[x]_\sim$: x∈A}, where $[x]_\sim$ = {y∈A: x~y} Proposition: The same-component relation w.r.t a partition is an equivalence relation Theorem Rel.2: If ~ is an equivalence relation on A, then A/~ is a partition of A	
Antisymmetry	Let R be a relation on set A. R is antisymmetric iff ∀x,y ∈ A (xRy ∧ yRx ⇒ x=y) OR ∀x,y ∈ A (x ≠ y) ⇒ ((x,y) ∈ R) ⇒ ((y,x) ∉ R)	Not antisymmetric: ∃x,y ∈ A (xRy ∧ yRx ∧ x≠y) Not symmetric ≢ antisymmetric
	∀x,y ∈ $\mathbb{Z}^+$, aRb ⇔ $a\mid b$ is antisymmetric (lecture 6 eg 19a)	∀x,y ∈ $\mathbb{Z}$, aRb ⇔ $a\mid b$ is not antisymmetric (lecture 6 eg 19b)
Partial Order Relations	Let R be a relation on set A. Then R is a partial order relation (or partial order) iff R is reflexive, antisymmetric and transitive A set A is a partially ordered set (poset) w.r.t a partial order relation R on A, denoted by (A, R)	- 2 partial order relations are ≤ relation on a set of real nums & ⊆ relation on a set of sets - ≼: general partial order and notation x ≼ y is read "x is curly less than or equal to y"
Hasse Diagrams	Let ≼ be a partial order on a set A. A Hasse diagram of ≼ satisfies the following condition ∀distinct x,y,m ∈ A: - If x ≼ y and no m ∈ A is s.t. x ≼ m ≼ y, then x is placed below y w a line joining them, else no line joins x and y 1. Remove loops at all vertices 2. Remove arrows whose existence is implied by the transitive property 3. Remove direction indicators on the arrows	
Comparability & Compatible	Suppose ≼ is a partial order relation on a set A, and a, b ∈ A - a, b are comparable iff either a ≼ b or b ≼ a. Otherwise, a and b are noncomparable - a, b are compatible if ∃ c ∈ A s.t. a ≼ c or b ≼ c **T5Q10**: In all partially ordered set, any 2 comparable elements are compatible	
Maximal / Minimal / Largest / Smallest Element	Let set A be partially ordered w.r.t a relation ≼ and c ∈ A 1. c is a maximal elem of A iff ∀x ∈ A, (x ≼ c) or (x and c are not comparable). i.e. ∀x ∈ A (c ≼ x ⇒ c = x) (nothing is above c) 2. c is a minimal elem of A iff ∀x ∈ A, (c ≼ x) or (x and c are not comparable). i.e. ∀x ∈ A (x ≼ c ⇒ c = x) 3. c is the largest elem of A iff ∀x ∈ A (x ≼ c) (c is above everything; largest elem need to be comparable w all other elems) 4. c is the smallest elem of A iff ∀x ∈ A (c ≼ x)	
	Consider a partial order ≼ on a set A.	A smallest elem is minimal. (Likewise, any largest elem is maximal)
Linearization	Let ≼ be a partial order on a set A. A linearization of ≼ is a total order $≼^*$ on A s.t ∀x,y ∈ A (x ≼ y ⇒ x $≼^*$ y)	Linearization of a partial order can be seen as deriving 1 total order (among other possible total orders) from that partial order
Total Order Relations	If R is a partial order relation on a set A, and for any 2 elems x,y in A, either xRy or yRx, then R is a total order relation (or total order) on A. i.e. R is a total order iff R is a partial order and ∀x,y ∈ A (xRy ∨ yRx)	Hasse diagram of a total order is 1 single line (chain). Linearization of a total order is the total order itself
Kahn's Algo	Input: A finite set A and a partial order ≼ on A Output: A linearization $≼^*$ of ≼, for all indices i,j $c_i ≼^* c_j$ ⇔ i ≤ j	1. Set A_0 := A and i := 0 2. Repeat until A_i = ∅ {2.1 find a minimal elem c_i of A_i w.r.t ≼; 2.2 set $A_{i+1} = A_i \setminus \{c_i\}$; 2.3 set i := i+1}
Well-Ordered Set	Let ≼ be a total order on a set A. A is well-ordered iff every non-empty subset of A contains a smallest elem. i.e. ∀S ∈ P(A), S = ∅ ⇒ (∃x ∈ S $\forall y$ ∈ S (x ≼ y))	Lecture 6 example 27 ($\mathbb{N}$, ≤) is well-ordered. ($\mathbb{Z}$, ≤) is not well-ordered

Function	A (well-defined) fn f from a set X to a set Y, denoted f:X → Y, is a relation satisfying 1) ∀x ∈ X, ∃y ∈ Y s.t. (x,y) ∈ f. 2) ∀x ∈ X, ∀y_1, y_2 ∈ Y, ((x,y_1) ∈ f ∧ (x,y_2) ∈ f) → y_1 = y_2 OR f:X → Y iff ∀x ∈ X, ∃!y ∈ Y s.t. (x,y) ∈ f (i.e. ea elem of X map to exactly 1 elem of Y)	For arrow diagram, 1) every elem of X has a arrow coming out of it. 2) no elem of X has 2 arrows coming out of it that points to 2 diff elem of Y

(Setwise) image & preimage	Let $f: X \to Y$ iff $(x,y) \in f$. So f maps x to y OR $x \xrightarrow{f} y$ OR $f: x \mapsto y$. x is called the argument of f f(x) is "f of x" OR output of f for input x OR value of f at x OR image of x under f. And x is a preimage of f(x)	If $A \subseteq X$, then let $f(A) = \{f(x): x \in A\}$, f(A) is the setwise image of A If $B \subseteq Y$, then let $f^{-1}(B) = \{x \in X: f(x) \in B\}$, $f^{-1}(B)$ is the setwise preimage of B under f $f^{-1}(B)$ is NOT an inverse fn. (elem in B might not have preimage)
Domain, co-domain, range	Let $f: X \to Y$ be a fn from set X to set Y X is domain of f and Y is co-domain of f.	Range of f is the (setwise) image of X under f. i.e $\{y \in Y: y = f(x) \text{ for some } x \in X\}$ Range ⊆ co-domain
Sequence & String	Seq $a_0, a_1, \ldots$ can be represented by a fn a whose domain is $\mathbb{Z}_{\geq 0}$ that satisfies $a(n) = a_n \ \forall n \in \mathbb{Z}_{\geq 0}$ Fibonacci seq $F_0, F_1, \ldots$ defined $\forall n \in \mathbb{Z}_{\geq 0}$, $F_0 = 0$, $F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$	
	Let A be a set. A string/word over A is of the form $a_0a_1 \ldots a_{l-1}$ where $l \in \mathbb{Z}_{\geq 0}$ and $a_0, a_1, \ldots, a_{l-1} \in A$ l is aka length of string. Empty string ε is string of length 0 Let A* denote set of all strings over A	
	Equality of Seq: Given 2 seq, defined by fn $a(n) = a_n$ and $b(n) = b_n \ \forall n \in \mathbb{Z}_{\geq 0}$, 2 seq are equal iff $a(n) = b(n) \ \forall n \in \mathbb{Z}_{\geq 0}$ Equality of Strings: Given 2 strings $s_1 = a_0a_1 \ldots a_{l-1}$ and $s_2 = b_0b_1 \ldots b_{l-1}$ where $l \in \mathbb{Z}_{\geq 0}$, $s_1 = s_2$ iff $a_i = b_i \ \forall n \in \{0,1,2,\ldots,l-1\}$	
Function equality	**Thrm 7.1.1** Fn Equality: 2 fn $f: A \to B$ and $g: C \to D$ are equal, f = g iff 1) A=C and B=D, and 2) $f(x) = g(x) \ \forall x \in A$	
Injections (One-to-One fn)	Fn $f: X \to Y$ is injective (one-to-one) iff $\forall x_1, x_2 \in A \ (f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$ OR $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$ (contrapositive) An injective fn is called an injection. (every elem in codomain has ≤1 arrow gg to it)	
Surjections (Onto fn)	Fn $f: X \to Y$ is surjective (onto) iff $\forall y \in Y \ \exists x \in X \ (y=f(x))$, i.e. every elem in co-domain has a preimage. So range = co-domain A surjective fn is called a surjection. (every elem in codomain has ≥1 arrow gg to it)	
Bijection (One-to-One correspondences)	Fn $f: X \to Y$ is bijective iff f is injective and surjective, i.e. $\forall y \in Y \ \exists! x \in X \ (y=f(x))$. A bijective fn is called a bijection/one-to-one correspondence. (every elem in codomain has exactly 1 arrow gg to it)	
Inverse Fn	Let $f: X \to Y$. Then $g: Y \to X$ is an inverse of f iff $\forall x \in X \ \forall y \in Y \ (y=f(x) \Leftrightarrow x=g(y))$ Proposition: Uniqueness of inverses: If g_1 and g_2 are inverses of $f: X \to Y$, then $g_1 = g_2$ **Thrm 7.2.3**: If $f: X \to Y$ is a bijection, then $f^{-1}: Y \to X$ is also a bijection. i.e. $f: X \to Y$ is bijective iff f has an inverse	
Composition of Fns	Let $f: X \to Y$ and $g: Y \to Z$ be fns. Define a new fn $g \circ f: X \to Z$ as $(g \circ f)(x) = g(f(x)) \ \forall x \in X$ $g \circ f$ is the composition of f and g (g circle f/g of f of x)	
Identity Fn	Identity fn on set X, id_X, if the fn from X to X defined as $id_X(x) = x \ \forall x \in X$ **Thrm 7.3.1** Composition w an Identity Fn: If f is a fn from set X to set Y, and id_X is the identity fn on X, and id_Y is the identity fn on Y, then $f \circ id_X = f$ and $id_Y \circ f = f$ **Thrm 7.3.2** Composition of Fn w its Inverse: If $f: X \to Y$ is a bijection w inverse fn $f^{-1}: Y \to X$, then $f^{-1} \circ f = id_X$ and $f \circ f^{-1} = id_Y$	
Properties	Thrm Associativity of Fn Composition: Let $f: A \to B$, $g: B \to C$ and $h: C \to D$. Then $(h \circ g) \circ f = h \circ (g \circ f)$ Fn composition is NONcommutative: $(g \circ f)(x) \neq (f \circ g)(x)$ **Thrm 7.3.3**: If $f: X \to Y$ and $g: Y \to Z$ are both injective, then $g \circ f$ is injective **Thrm 7.3.4**: If $f: X \to Y$ and $g: Y \to Z$ are both surjective, then $g \circ f$ is surjective **T6Q6**: If $g \circ f$ is injective, $f: X \to Y$ and g has domain Y, then f is injective **T7Q7**: If $f \circ g$ is surjective, $f: X \to Y$ and g has codomain X, then f is surjective	
$\mathbb{Z}_n$	Quotient $\mathbb{Z}/\sim_n$ where $\sim_n$ is the congruence-mod-n relation on $\mathbb{Z}$, is denoted $\mathbb{Z}_n$ E.g. $\mathbb{Z}_2 = \{\{2k: k \in \mathbb{Z}\}, \{2k+1: k \in \mathbb{Z}\}\}$ Define addition + and multiplication · on $\mathbb{Z}_n$ as: whenever $[x], [y] \in \mathbb{Z}_n$, $[x] + [y] = [x+y]$ and $[x] \cdot [y] = [x*y]$ Proposition: Addition on $\mathbb{Z}_n$ is well defined. For all $n \in \mathbb{Z}^+$ and all $[x_1],[y_1],[x_2],[y_2] \in \mathbb{Z}_n$, $[x_1] = [x_2]$ and $[y_1] = [y_2] \Rightarrow [x_1] + [y_1] = [x_2] + [y_2]$ Proposition: Multiplication on $\mathbb{Z}_n$ is well defined. For all $n \in \mathbb{Z}^+$ and all $[x_1],[y_1],[x_2],[y_2] \in \mathbb{Z}_n$, $[x_1] = [x_2]$ and $[y_1] = [y_2] \Rightarrow [x_1] \cdot [y_1] = [x_2] \cdot [y_2]$	
Order of Bijection	The order of a bijection $f: X \to X$ is defined to be the least $n \in \mathbb{Z}^+$ s.t. $f \circ f \circ \ldots \circ f = id_A$ (n times of f)	

Sequences	Seq is an ordered set w members called terms. General form: $a_m, a_{m+1}, \ldots, a_n$ where m ≤ n Explicit form: $a_k = f(k)$ where f is some fn Summation: $\sum_{k=m}^{n} a_k$. Expanded form of sum: $a_m + a_{m+1} + \ldots + a_n$ Summation using recursion: $\sum_{k=m}^{n} a_k = \sum_{k=m}^{n-1} a_k + a_n$, for all integers n > m	By convention if m > n, then summation = 0 Telescoping sums: convert to partial fractions If m > n, $\prod_{m}^{n} a_k = 1$
Common seq	Arithmetic seq/progression iff there is a constant d s.t. $a_k = a_{k-1} + d$, $\forall k \in \mathbb{Z}^+$. So $a_n = a_0 + nd$, ∀ ints n ≥ 0 Geometric seq/progression iff there is a constant r s.t. $a_k = ra_{k-1}$, $\forall k \in \mathbb{Z}^+$. So $a_n = a_0r^n$ ∀ ints n ≥ 0 Triangle nums: 1,3,6,10,15,21,28,... ; Fibonacci nums: 1,1,2,3,5,8,13,21,34,55,... Lazy Caterer's Seq: 1,2,4,7,11,16,... ; Catalan's nums: 1,1,2,5,14,42; $\frac{1}{n+1}\binom{2n}{n}$	$\sum_{k=0}^{n} a_k = \frac{n}{2}(2a_0 + (n-1)d)$ $\sum_{k=0}^{n-1} a_k = a_0\left(\frac{1-r^n}{1-r}\right)$ Note fn on right is known as closed form
Mathe-matical Induction	Principle of (weak/regular) Mathematical Induction (PMI/1PI) 1. $\forall n \in \mathbb{Z}^+$, let $P(n) \equiv \ldots$ 2. Basis step: Show P(a) is true 3. Inductive step: 3.1. Let $k \in \mathbb{Z}_{\geq a}$ s.t. P(k) is true, i.e. 3.2. Show P(k+1) true 5. $\forall n \in \mathbb{Z}^+$, P(n) true by MI	Strong Induction (2PI) 1. $\forall n \in \mathbb{Z}^+$, let $P(n) \equiv \ldots$ 2. Basis step: Show P(a) is true, P(a+1),... P(b) true 3. Inductive step: 3.1. Let $k \in \mathbb{Z}_{\geq a}$ s.t. P(a), P(a+1),... P(k + b-a) is true 3.2. Show P(k+1) true 5. $\forall n \in \mathbb{Z}^+$, P(n) true by Strong MI
Well-ordering Principle	Well-Ordering Principle for Integers: Every nonempty subset of $\mathbb{Z}_{\geq 0}$ has a smallest element.	
Recursively Defined Sets	Base clause: Specify certain elements, called founders are in S Recursion clause: Specify certain constructors under which set S is closed Minimality clause: Membership for S can always be demonstrated by (infinitely many) successive applications of the clauses above	E.g. () is in P a. If E is in P, so is (E); b. If E and F in P, so is EF
Structural Induction	To prove ∀ x ∈ S P(x) is true, suffices to (basis step) show P(c) is true for every founder c; and (induction step) show ∀ x ∈ S (P(x) → P(f(x)) is true for every constructor f	x ∈ S by base clause y ∈ S by recursion clause w n = ...
Thrm 5.1.1	If $a_m, a_{m+1}, \ldots$ and $b_m, b_{m+1}, \ldots$ are seq of real nums and c is any real num, then for any int n ≥ m: 1. $\sum_{k=m}^{n} a_k + \sum_{k=m}^{n} b_k = \sum_{k=m}^{n}(a_k + b_k)$ 2. $c \cdot \sum_{k=m}^{n} a_k = \sum_{k=m}^{n} c \cdot a_k$ (generalized distributive law) 3. $(\prod_{m}^{n} a_k) \cdot (\prod_{m}^{n} b_k) = (\prod_{m}^{n}(a_k \cdot b_k))$	
Theorem 5.2.2	Sum of 1st n ints: For all ints n ≥ 1, $1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$	

Theorem 5.2.3	Sum of GP: For any real num r ≠ 1, and any int n ≥ 0, $\sum_{i=0}^{n} r^i = \frac{1-r^{n+1}}{1-r}$	Some fact from tutorial: Product of any 2 consecutive integers is even	
Proposition 5.3.1	For all ints n ≥ 0, $2^{2n} - 1$ is divisible by 3	**Proposition 5.3.2**	For all ints n ≥ 3, $2n + 1 < 2^n$
T7Q1	$\sum_{i=1}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$	**T7Q2**	Let $x \in \mathbb{R}_{\geq 1}$. $\forall$ $n \in \mathbb{Z}^+$, $1 + nx \leq (1+x)^n$

Pigeonhole Principle	Let A and B be finite sets. If there is an injection f: A → B, then |A| ≤ |B|
Dual Pigeonhole Principle	Let A and B be finite sets. If there is a surjection f: A → B, then |A| ≥ |B|
Cardinality	Let $\mathbb{Z}_n$ = {1,2,3,...,n}. Set S is finite iff S is empty or ∃ a bijection from S to $\mathbb{Z}_n$ for some $n \in \mathbb{Z}^+$ Cardinality of a finite set S, |S| is $\begin{cases} 0, \text{if } S = \emptyset \\ \text{n, if f}: S \to \mathbb{Z}_n \text{ is a bijection} \end{cases}$ A set S is infinite if it is not finite Theorem: Equality of Cardinality of Finite Sets: Let A and B be any finite sets. |A| = |B| iff there is a bijection f: A → B Same Cardinality (Cantor): Given any 2 sets A and B. A have same cardinality as B, |A| = |B| iff there is a bijection f: A → B **Thrm 7.4.1** Properties of Cardinality: The cardinality is an equivalence relation For all sets A,B and C: Reflexive: |A| = |A|. Symmetric: |A| = |B| → |B| = |A| Transitive: (|A| = |B|) ∧ (|B| = |C|) → |A| = |C|
Countably Infinite	Cardinal numbers: Define $\aleph_0 = \lvert\mathbb{Z}^+\rvert$ *or* $\lvert\mathbb{Z}_{\geq 0}\rvert$ ("aleph"; 1st cardinal number) A set S is countably infinite (or S has the cardinality of natural numbers) iff |S| = $\aleph_0$ A set is countable iff it is finite or countably infinite A set is uncountable if it is not countable
Eg	$\mathbb{Z}$ is countable. Let f(n): $\mathbb{Z}^+ \to \mathbb{Z}$ = $\begin{cases} n/2, \textit{if n is even positive int} \\ -(n-1)/2, \textit{if n is odd positive int} \end{cases}$ $\mathbb{Q}^+$ is countable. Set F(1) = $\frac{1}{1}$, F(2) = $\frac{1}{2}$, F(3) = $\frac{2}{1}$, F(4) = $\frac{3}{1}$, Then skip $\frac{2}{2}$ since counted, F(5) = $\frac{1}{3}$ Every positive rational num appears somewhere in grid, and counting procedure is so every point in grid is reached eventually. Thus F is surjective Skipping numbers that have already been counted ensures no num is counted twice. F is injective. So F is a bijection from $\mathbb{Z}^+$ to $\mathbb{Q}^+$. So $\mathbb{Q}^+$ is countably infinite and countable. Thrm: $\mathbb{Z}^+ \times \mathbb{Z}^+$ is countable. Set f: $\mathbb{Z}^+ \times \mathbb{Z}^+ \to \mathbb{Z}^+$: f(x,y) = $\frac{(x+y-2)(x+y-1)}{2} + x$ 
Theorems	Cartesian Product: If sets A and B are both countably infinite, then so is $A \times B$ Corollary (General Cartesian Product): Given n ≥ 2 countably infinite sets $A_1, A_2, ..., A_n$, $A_1 \times A_2 \times ... \times A_n$ is also countably infinite Thrm (Unions): The union of countably many countable sets is countable. i.e. if A_1, A_2, ... are all countable sets, then so is $\bigcup_{i=1}^{\infty} A_i$
Countability via Sequences	**Proposition 9.1** An infinite set B is countable iff there is a seq $b_0, b_1, ... \in B$ in which every element of B appears exactly once **Lemma 9.2** (Countability via Sequence): An infinite set B is countable iff there is a seq $b_0, b_1, ... \in B$ in which every element of B appears
Larger Infinities	**Thrm 7.4.2 (Cantor):** The set of real numbers btw 0 and 1 is uncountable Cantor's Diagonalization Argument (Proof by contradiction): 1. Suppose (0,1) is countable 2. Since it is not finite, it is countably infinite 3. List the elems x_i of (0,1) in a seq as follows: $x_1 = 0.a_{11}a_{12}a_{13}...a_{1n}...$, $x_2 = 0.a_{21}a_{22}a_{23}...a_{2n}...$, $x_3 = 0.a_{31}a_{32}a_{33}...a_{3n}...$, ⋮ $x_n = 0.a_{n1}a_{n2}a_{n3}...a_{nn}...$, ⋮ 4. Construct a num $d = 0.d_1d_2d_3...d_n...$ s.t. $d_n = \begin{cases} 1, \textit{if } a_{nn} \neq 1 \\ 2, \textit{if } a_{nn} = 1 \end{cases}$ 5. Note that $\forall n \in \mathbb{Z}^+$, $d_n \neq a_{nn}$. Thus $d \neq x_n$ $\forall n \in \mathbb{Z}^+$ 6. But d ∈ (0,1), hence contradiction. Thus (0,1) uncountable
Thrms	**Thrm 7.4.3:** Any subset of any countable set is countable **Corollary 7.4.4**: Any set w an uncountable subset is uncountable. Since (0,1) ⊆ $\mathbb{R}$, $\mathbb{R}$ 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 ∪ B is countable
Cardinality of $\mathbb{R}$	|$\mathbb{R}$| = |(0,1)|. Let S = (0,1). Imagine picking up S and bending it into a circle Define F: S → $\mathbb{R}$ as follows: Draw a number line and place S bent into a circle, tangent to the line above point 0 For each point x on the circle representing S, draw a straight line L through the topmost point of the circle and x Let F(x) be the pt of intersection of L and the number line Can be seen that F(x) is injective and surjective. Hence S and $\mathbb{R}$ have same cardinality 
T8Q2	Let B be a countably infinite set and C be a finite set, then B ∪ C is countable
T8Q4	Suppose A_1, A_2,... are countable sets. Then $\bigcup_{i=1}^{n} A_i$ is countable for any $n \in \mathbb{Z}^+$
T8Q7	Set B is infinite iff ∃ A ⊊ B s.t. |A| = |B|
T8Q9	Let A be a countably infinite set. Then $\mathcal{P}$(A) is uncountable

Probability & Counting	Equally Likely Probability Formula: If S is a finite sample space where all outcomes are equally likely and E is an event in S, then the probability of E, P(E) = $\frac{\textit{num of outcomes in E}}{\textit{total num of outcomes in S}} = \frac{\lvert E\rvert}{\lvert S\rvert}$ **Thrm 9.1.1** Number of elements in a list: If m and n are integers and m ≤ n, then there are n-m+1 integers from m to n inclusive E.g. how many ints divisible by 5 from 100 to 999: 100 = 5*20, 995 = 5*199. So 199-20+1 = 180 such ints
Product/ multiplication rule	**Thrm 9.2.1** (Multiplication/Product Rule): If an operation consists of k steps and 1st step can be performed in n_1 ways, 2nd step in n_2 ways, ... kth step in n_k ways (regardless of preceding steps), then entire op can be performed in $n_1 * n_2 * ... * n_k$ ways **Thrm 5.2.4** (Sets): Suppose A is a finite set. Then $\lvert\wp(A)\rvert = 2^{\lvert A\rvert}$
Addition/ sum rule	**Thrm 9.3.1** (Addition/Sum rule): Suppose a finite set A equals the union of k distinct mutually disjoint subsets $A_1, A_2, ..., A_k$. Then |A| = $\lvert A_1\rvert + \lvert A_2\rvert + ... + \lvert A_k\rvert$
Permutation	Permutation is an ordering of the objects in a row. **Thrm 9.2.2** (Permutations): The num of permutations of a set with n (n ≥ 1) elements is n! **Thrm 9.2.3** (r-permutations from a set of n elements): If n and r are ints and 1 ≤ r ≤ n, then the num of r-permtations of a set of n elems is P(n,r) = n(n-1)(n-2)...(n-r+1) = $\frac{n!}{(n-r)!}$
Difference rule	**Thrm 9.3.2** (Difference Rule): If A is a finite set and B ⊆ A, then |A\\B| = |A| – |B| Formula for Probability of the Complement of an Event: If S is a finite sample space and A is an event in S, then P($\bar{A}$) = 1 – P(A)
Inclusion/ Exclusion Rule	**Thrm 9.3.3** (Inclusion/Exclusion Rule for 2 or 3 sets): If A, B, and C are any finite sets, then |A∪B| = |A| + |B| – |A∩B| and |A∪B∪C| = |A| + |B| + |C| – |A∩B| – |A∩C| – |B∩C| + |A∩B∩C|

Pigeonhole Principle (PHP)	A function from one finite set to a smaller finite set cannot be one-to-one (injective): There must be at least 2 elements in the domains that have the same image in co-domain	
	Application to Decimal Expansions of Fractions: Decimal expansion of any rational num either terminates or repeats	
	Generalised Pigeonhole Principle: For any fn f from a finite set X w n elems to a finite set Y w m elems and for any positive int k, if k < n/m, there there is some y ∈ Y s.t. y is the image of at least k+1 distinct elems of X	
	Generalized Pigeonhole Principle (**Contrapositive Form**): For any fn f from a finite set X w n elems to a finite set Y w m elems and for any positive int k, if for each y ∈ Y, $f^{-1}(\{y\})$ has at most k elems, then X has at most km elems; i.e. n ≤ km	
Combinations	Let n and r be nonnegative ints w r ≤ n. An r-combination of a set n elems is a subset of r of the n elem. $\binom{n}{r}$ denotes num of subsets of size r that can be chosen from set of n elems **Thrm 9.5.1** Formula for $\binom{n}{r}$: $\binom{n}{r} = \frac{n!}{r!(n-r)!}$, where n and r are nonnegative ints w r ≤ n	r- permutation: Ordered selection r-combination: unordered selection P(n,r) = $\binom{n}{r}$ * r!
Repetitions allowed	**Thrm 9.5.2** Permutations w Sets of Indistinguishable Objs: Suppose a collection consists of n objs of which n_1 are of type 1 and are indistinguishable from ea other, n_2 are of type 2 and are indistinguishable from ea other,..., n_k are of type k and are indistinguishable from ea other and suppose $n_1 + n_2 + ... + n_k = n$. Then num of distinguishable permutations of the n objs is $\binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\cdots\binom{n-n_1-n_2-\cdots-n_{k-1}}{n_k} = \frac{n!}{n_1!n_2!n_3!\ldots n_k!}$	
	An r-combination w repetition allowed OR multiset of size r, chosen from a set X of n elems is an unordered selection of elems taken from X w repetition allowed. Note objects are indistinguishable If X = $\{x_1,x_2,...,x_n\}$, multiset of size r is $[x_{i_1}, x_{i_2}, \ldots, x_{i_r}]$ where ea x_{i_j} is in X and some of the x_{i_j} may equal ea other Thrm 9.6.1 Num of r-combinations w repetition: Num of multisets of size r that can be selected from a set of n elems is $\binom{n+r-1}{r}$ Num of soln to $x_1 + x_2 + ... + x_n = r$, x_i is nonnegative int: $\binom{r+(n-1)}{r}$ Num of soln to $x_1 + x_2 + x_3 = 20$, x_i is a positive int: equivalent to $y_1 + y_2 + y_3 = 17$: $\binom{3+17-1}{17} = \binom{n-1}{r}$	

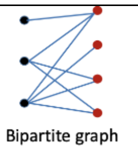
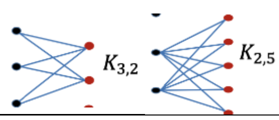
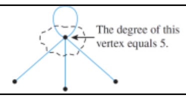
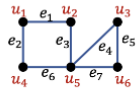
Summary

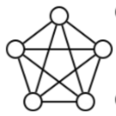
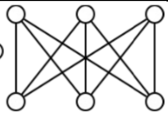
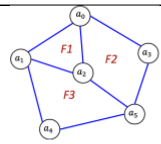
	Order Matters	Order don't matter
Repetition	n^k	$\binom{n+k-1}{k}$
No Repetition	P(n,k)	$\binom{n}{k}$

Circular Permutation of n objects is (n-1)!

Pascal's Formula	**Thrm 9.7.1** Pascal's Formula: Let n and r be positive ints, r ≤ n. Then $\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$ Combinatorial Proof uses counting as basis of proof. Includes bijective proof and proof by double counting (counting num of elems in 2 diff ways to obtain diff expressions in identity) For 0 ≤ k ≤ n, $\binom{n}{r} = \binom{n}{n-r}$ (don't choose n-r ppl) For 0 ≤ k ≤ n, k$\binom{n}{k}$ = n$\binom{n-1}{k-1}$ (choose k committee & chairperson) $2^n = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n}$ (num of subsets of power set)	
Binomial Theorem	**Thrm 9.7.2** Binomial Thrm: Given any real nums a and b and any non-negative int 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 fn P from set of all events in S to set of real nums satisfies the following axioms: For all events A and B in S,	1. 0 ≤ P(A) ≤ 1 2. P(∅) = 0 and P(S) = 1 3. If A and B are disjoint events (A∩B=∅), then P(A∪B) = P(A) + P(B)
Formula	Probability of Complement: If A is any event in sample space S, then P($\bar{A}$) = 1 – P(A) Probability of General Union of 2 events: If A and B are any events in sample space S, then P(A∪B) = P(A) + P(B) – P(A∩B) Suppose possible outcomes of an experiment are real nums $a_1,a_2,...,a_n$ w prob $p_1,p_2,...,p_n$. The expected value is $\sum_{k=1}^{n} a_k p_k$ Linearity of Expectation: $E[\sum_{i=1}^{n} c_i X_i] = \sum_{i=1}^{n}(c_i \cdot E[X_i])$	
Conditional Probability	If P(A) ≠ 0, then conditional prob of B given A, P(B|A) = $\frac{P(A\cap B)}{P(A)}$ OR $P(A\cap B)$ = P(B|A)*P(A) OR P(A) = $\frac{P(A\cap B)}{P(B\|A)}$	
Bayes Theorem	**Thrm 9.9.1** Bayes Thrm: Suppose sample space S is a union of mutually disjoint events $B_1, B_2, ..., B_n$ Suppose A is an event in S, and suppose A and all the B_i have non-zero prob. If k is an int w 1 ≤ k ≤ n, then $P(B_k\|A) = \frac{P(A\cap B_k)}{P(A)} = \frac{P(A\|B_k)*P(B_k)}{P(A\|B_1)*P(B_1)+P(A\|B_2)*P(B_2)+\ldots+P(A\|B_n)*P(B_n)}$	
Independent Events	If A and B are events in sample space S, then A and B are indep iff P($A\cap B$) = P(A) * P(B)	
Pairwise independent/ Mutually Independent	Let A,B and C be events in sample space S. A,B and C are pairwise indep, iff they satisfy conditions 1–3. They are mutually independent iff they satisfy all 4 conditions	
	1. P($A\cap B$) = P(A)*P(B)	3. P($B\cap C$) = P(B) * P(C)
	2. P($A\cap C$) = P(A)*P(C)	4. P($A\cap B\cap C$) = P(A)*P(B)*P(C)
	Events $A_1,A_2,...,A_n$ in sample space S are mutually indep iff probability of intersection of any subsets of events is the product of probabilities of the events in the subset	
Binomial Dist	X~Binomial(n,p). P(X=x) = $\binom{n}{x} p^x (1-p)^x$	

Undirected Graph	Undirected graph is denoted by G = (V,E), where V= $\{v_1,...,v_n\}$ is set of vertices/nodes in G and E = $\{e_1,...,e_k\}$ is set of (undirected) edges in G An (undirected) edge e connecting v_i and v_j is denoted as e = $\{v_i,v_j\}$ (i can = j) An undirected graph G consists of 2 finite sets: a nonepty set V of vertices and a set E of edges, where each (undirected) edge is associated w a set consisting of either 1 or 2 vertices called its endpoints An edge connect its endpoints; vertext that is an endpoint of a loop is aka adjacent to itself; and 2 vertices connected by an edge aka adjacent vertices An edge is incident on each of its endpoints, and 2 edges incident on the same endpoint are called adjacent edges
Directed Graph	Directed graph/digraph G consists of 2 finites 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 e = (v,w) for a directed edge e from vertex v to vertex w
Simple Graph	Simple graph is an undirected graph that does not have any loops (edge to itself) or parallel edges (both with same set of vertices). (i.e. there is at most 1 edge btw each pair of distinct vertices)

Complete Graph	A complete graph on n vertices, n > 0, denoted K_n is a simple graph w n vertices and exactly 1 edge connecting each pair of distinct vertices Number of edges = $\frac{(n-1)(n)}{2}$
Bipartite Graph	Bipartite graph/bigraph is a simple graph whose vertices can be divided into 2 disjoint sets U and V s.t. every edge connects a vertex in U to 1 in V Complete Bipartite graph is a bipartite graph on 2 disjoint set U and V s.t. every vertex in U connects to every vertex in V. If |U| = m and |V| = n, the complete bigraph is denoted as $K_{m,n}$  Complete bipartite 
Subgraph of Graph	A graph H is a subgraph of graph G iff every vertex in H is also a vertex in G and every edge in H is also an edge in G, and every edge in H has the same endpoints as it has in G
Degree of a Vertex	Let G be a undirected graph and v a vertex of G. The degree of v, deg(v) = num of edges that are incident on v, w an edge that is a loop counted twice The total degree of G = sum of degress of all vertices of G 
Thrm for undirected graph?	**Thrm 10.1.1** Handshake Theorem: If G is any graph, then the sum of degrees of all vertices = 2*num of edges of G **Corollary 10.1.2**: The total degree of a graph is even **Proposition 10.1.3**: In any graph, there are an even num of vertices of odd degree
Indegree & Outdegree	Let G = (V,E) be a directed graph and v a vertex of G. The indegree of v, $deg^-(v)$ is num of directed edges that end at v. The outdegree of v, $deg^+(v)$ = num of directed edges that originate from v Note $\sum_{v \in V} deg^-(v) = \sum_{v \in V} deg^+(v) = \|E\|$
Travel in a graph	Let G be a graph and v and w be vertices of G. A **walk** from v to w is a finite alternating sequence of adjacent vertices and edges of G. A walk has the form $v_0e_1v_1e_2,...,v_{n-1}e_nv_n$, where v's are vertices, e are edges, v_0 = v, v_n = w, and ∀ i ∈ {1,2,...,n}, v_{i-1} and v_i are the endpoints of e_i. The num of edges, n, is the **length** of the walk The **trivial walk** from v to v consists of the single vertex v A **trail** from v to w is a walk from v to w that does not contain a repeated edge A **path** from v to w is a trail that does not contain a repeated vertex A **closed walk** is a walk that starts and ends at the same vertex A **circuit/cycle** is a closed walk of length at least 3 that does not contain a repeated edge A **simple circuit/cycle** is a circuit that does not have any other repeated vertex except the first and last An undirected grph is **cyclic** if it contains a loop or a cycle; otherwise it is acyclic  $u_1e_1u_2e_3u_5e_4u_3e_5u_6e_7u_5e_3u_2$ is a walk (may repeat edges and/or vertices) $u_1e_1u_2e_3u_5e_4u_3e_5u_6e_7u_5e_6u_4$ is a trail (cannot repeat edges) $u_1e_1u_2e_3u_5e_4u_3e_5u_6$ is a path (cannot repeat vertices and edges) $u_5e_6u_4e_2u_1e_1u_2e_3u_5e_7u_6e_5u_3e_4u_5$ is a circuit $u_5e_6u_4e_2u_1e_1u_2e_3u_5$ is a simple circuit
Connected-ness	2 vertices v and w of graph G = (V,E) are connected iff there is a walk from v to w The graph 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 2 distinct vertices of G can be connected by a path b) If vertices v and w are part of a circuit in G and 1 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 w/o disconnecting G
Connected Component	A graph H is a connected component of a graph G iff 1. The graph H is a subgraph of G 2. The graph H is connected 3. No connected subgraph of G has H as a subgraph and contains vertices or edges that are not in H ("largest size/can be expanded")
Euler Circuits	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 An Eulerian graph is a graph that contains an Euler circuit **Thrm 10.2.2**: If a graph has an Euler circuit, then every vertex of the graph has positive even degree Contrapositive of Thrm 10.2.2: if some vertex of a graph has odd degree, then the graph does not have an Euler circuit **Thrm 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 **Thrm 10.2.4**: A graph G has an Euler circuit iff G is connected and every vertex of G has positive even degree **Euler Trail**: Let G be a graph, and v and w be 2 distinct vertices of G. An Euler trail/path from v to w is a seq of adjacent edges and vertices that starts at v, ends at w, passes through every vertex of G at least once, and traverses every edge of G exactly once **Corollary 10.2.5**: Let G be a graph, and v and w be 2 distinct vertices of G. There is an Euler trail from v to w iff G is connected, v and w have odd degree, and all other vertices of G have positive even degree
Hamiltonian Circuits	Given a graph G, a Hamiltonian circuit for G is a simple circuit that includes every vertex of G (i.e. every vertex appears exactly once, except for the first and last which are the same) A Hamiltonian/Hamilton graph is a graph that contains a Hamiltonian circuit Euler circuit can visit vertices more than once. Hamiltonian circuit 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 w the following properties: 1. H contains every vertex of G. 2. H is connected. 3. H has the same num of edges as vertices. 4. Every vertex of H has deg 2 Contrapositive of 10.2.6 says if a graph G does not have a subgraph H w properties (1)-(4), then G does not have a Hamiltonian circuit
Matrix	$\mathbf{A}_{m \times n} = (a_{ij})$. **A** = **B** iff A and B have the same size, and $a_{ij} = b_{ij}$ ∀ i = 1,2,...,m and j = 1,2,...,n Square matrix: matrix w same num of rows and cols If A is a sq matrix of size n x n, then main diagonal of A consists of entries $a_{11}, a_{22}, ..., a_{nn}$ Let G be a directed graph w ordered vertices $v_1,...,v_n$. The adjacency matrix of G is the n x n matrix **A** = (a_{ij}) over the set of non-negative ints s.t. a_{ij} = num of arrows from v_i to v_j ∀ i,j = 1,2,...,n Let G be an undirected graph w ordered vertices $v_1,...,v_n$. The adjacency matrix of G is the n x n matrix **A** = (a_{ij}) over the set of non-negative ints s.t. a_{ij} = num of edges connecting v_i and v_j ∀ i,j = 1,2,...,n Note adjacency matrix for undirected graph is symmetric (i.e. $a_{ij} = a_{ji}$)
	Let A = (a_{ij}) be m x k matrix, B = (b_{ij}) be k x n matrix. AB is the matrix (c_{ij}) where $c_{ij} = \sum_{r=1}^{k} a_{ir}b_{rj}$ ∀i = 1,...,m and j = 1,...,n Note matrix multiplication is NOT commutative. Matrix multiplication is associative For each positive int n, the n x n identity matrix, denoted $I_n = (\delta_{ij})$ or just **I**, where $\delta_{ij} = \begin{cases} 1, if\ i = j \\ 0, if\ i \neq j \end{cases}$, ∀i,j = 1,2,...n For any n x n matrix A, the powers of A are: $A^0 = I$. $A^n = AA^{n-1}$
	Thrm 10.3.2: If G is a graph w vertices $v_1,...v_m$ and **A** is the adjacency matrix of G, then for each positive int n and ∀ ints i,j = 1,2,...,m, the ij^{th} entry of $\mathbf{A}^n$ = num of walks of length n from v_i to v_j

Isomor-phism	Let G = (V_G, E_G) and G' = ($V_{G'}$, $E_{G'}$) be 2 graphs. G is isomorphic to G', G ≅ G', iff there exists bijections g: $V_G \rightarrow V_{G'}$ and h: $E_G \rightarrow E_{G'}$ that preserve the edge-endpoint functions of G and G' in the sense that ∀ v ∈ V_G and e ∈ E_G, v is an endpoint of e ⇔ g(v) is an endpoint of h(e) OR G is isomorphic to G' iff there exists a permutation π: $V_G \rightarrow V_{G'}$ s.t. {u,v} ∈ E_G ⇔ {π(u),π(v)} ∈ $E_{G'}$ **Thrm 10.4.1** Graph Isomorphism is an Equivalence Relation: Let S be a set of graphs and let ≅ be the relation of graph isomorphism on S. Then ≅ is an equivalence relation on S	
Planar Graphs	A planar graph is a graph that can be drawn on a (2D) plane w/o edges crossing Kuratowski's Thrm: A finite graph is planar iff it does not contain a subgraph that is a subdivision of the complete graph K_5 or the complete bipartite graph $K_{3,3}$ Euler's Formula: For a connected planar simple graph G = (V,E) w e = |E| and v = |V|, if we let f be number of faces/regions, then f = e - v + 2	 K_5  $K_{3,3}$  F4 (F4 = 'outside' the planar graph) e = 8, v = 6, f = 8-6+2 = 4
Complement Graph	If G is a simple graph, the complement of G, denoted $\bar{G}$, is obtained as follows: the vertex set of $\bar{G}$ is identical to the vertex set of G. However, two distinct vertices v and w of $\bar{G}$ are connected by an edge if and only if v and w are not connected by an edge in G.	
	A self-complementary graph is isomorphic w 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).	

Tree	(graph is assumed to be undirected) Graph is **circuit-free** iff it has no circuit Graph is a **tree** iff it is circuit-free and connected **Trivial tree** is a graph that has only a single vertex	Graph is a **forest** iff circuit free and not connected Let T be a tree. If T has only 1 or 2 vertices, then each is called a **terminal vertex/leaf**. If T has at least 3 vertices, then a vertex of deg 1 in t is a terminal vertex/leaf, and a vertex of deg > 1 in T is an internal vertex
	Lemma 10.5.1: Any non-trivial tree has at least 1 vertex of deg 1 **Thrm 10.5.2**: Any tree w n vertices (n > 0) has n - 1 edges (proof by MI) A non-trivial tree has at least 2 vertices of deg 1 **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. **Thrm 10.5.4**: If G is a connected graph w n vertices and n-1 edges, then G is a tree	Proof 10.5.1. Let T be a arbitrarily chosen non-trivial tree 1. Pick a vertex v of T and let e be an edge incident on v 2. While deg(v) > 1, repeat step 2a, 2b and 2c: 2a. Choose e' to be an edge incident on v s.t. e' ≠ e 2b. Let v' be the vertex at other end of e' from v 2c. Let e = e' and v = v' Algo must eventually terminate as set of vertices of T is finite and T is circuit-free. When it does, a vertex of deg 1 is found
Rooted Tree	**Rooted Tree** is a tree in which there is one vertex that is distinguished from the others and called the root **Level** of a vertex is num of edges along the unique path btw it and the root **Height** of a rooted tree is the max level of any vertex of the tree Given the root or any internal vertex v of a rooted tree, the **children** of v are all those vertices that are adjacent to v and are one level farther away from the root than v If w is a child of v, then v is the **parent** of w, and 2 distinct vertices that are both children of the same parent are called **siblings** Given 2 distinct vertices v and w, if v lies on the unique path btw w and the root, then v is an **ancestor** of w, and w is a **descendant** of v	
Binary Trees	A **binary tree** is a rooted tree in which every parent has at most 2 children. Each child is designated either a left child or a right child (but not both), and every parent has at most 1 left child and 1 right child. A **full binary tree** is a binary tree in which each parent has exactly 2 children Given any parent v in a binary tree T, if v has a left child, the the **left subtree** of v is the binary tree whose root is the left child of v, whoses 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.	
	Thrm 10.6.1: Full Binary Tree Thrm: If T is a full binary tree w k internal vertices, then T has a total of 2k+1 vertices and has k+1 terminal vertices (leaves) **Thrm 10.6.2**: For non-negative integers h, if T is any binary tree w height h and t terminal vertices (leaves), then $t \leq 2^h$ or equivalently, $h \leq \log_2 t$ (proof by strong MI)	
Tree Search	Tree search/traversal is process of visiting each node in a tree data structure exactly once in a systematic manner	
	BFS: Starts at root -> visits adjacent vertices -> move to next level	
	DFS: Pre-order	Print current vertex -> Traverse left subtree by recursively calling the pre-order fn -> Traverse right subtree by recursively calling the pre-order fn
	DFS: In-order	Traverse left subtree by recursively calling the in-order fn -> Print current vertex -> Traverse right subtree by recursively calling the in-order fn
	DFS: Post-order	Traverse left subtree by recursively calling the post-order fn -> Traverse right subtree by recursively calling the post-order fn -> Print current vertex
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 2 spanning trees for a graph have the same num of edges	
	A **weighted graph** is a graph for which each edge has an associated positive real num **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 weight of e and **w(G)** denotes the total weight of G	
Algos	Algo 10.7.1 Kruskal Input: G [a connected weighted graph w n vertices] 1. Initialise T to have all vertices of G and no edges 2. Let E be the set of all edges of G, and let m = 0 3. While (m < n-1): 3a. Find an edge e in E of least weight 3b. Delete e from E 3c. If addition of e to the edge set of T does not produce a circuit, then add e to edge set of T and set m = m+1 Output: T [T is a MST for G]	Algo 10.7.2 Prim Input: G [a connected weighted graph w n vertices] 1. Pick a vertex v of G and let T be the graph w this vertex only 2. Let V be the set of all vertices of G except v 3. For i = 1 to n-1: 3a. Find an edge e of G s.t. (1) e connects T to one of the vertices in V, and (2) e has the least weight of all edges connecting T to a vertex in V. Let w be the endpoint of e that is in V 3b. Add e and w to the edge and vertex sets of T, and delete w from V Output: T [T is a MST for G]