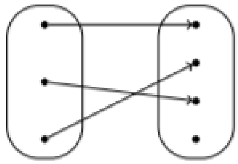
No.	Definition	Denotation	Description
			Logical Form and Logical Equivalence
2.1.1	Statement		A **statement** (or **proposition**) is a sentence that is true or false, but not both.
2.1.2	Negation	$\sim p$	If p is a statement variable, the **negation** of p is "not p" or "it is not the case that p" and is denoted $\sim p$.
2.1.3	Conjunction	$p \wedge q$	If p and q are statement variables, the **conjunction** of p and q is "p and q", denoted $p \wedge q$.
2.1.4	Disjunction	$p \vee q$	If p and q are statement variables, the **disjunction** of p and q is "p or q", denoted $p \vee q$.
2.1.5	Statement Form / Propositional Form		A **statement form** (or **propositional form**) is an expression made up of statement variables and logical connectives that becomes a statement when actual statements are substituted for the component statement variables.
2.1.6	Logical Equivalence	$\boldsymbol{P \equiv Q}$	Two statement forms are called **logically equivalent** if, and only if, they have identical truth values for each possible substitution of statements for their statement variables. The logical equivalence of statement forms P and Q is denoted by $\boldsymbol{P \equiv Q}$.
2.1.7	Tautology	t / true	A **tautology** is a statement form that is always true regardless of the truth values of the individual statements substituted for its statement variables. A statement whose form is a tautology is a **tautological statement**.
2.1.8	Contradiction	c / false	A **contradiction** is a statement form that is always false regardless of the truth values of the individual statements substituted for its statement variables. A statement whose form is a contradiction is a **contradictory statement**.
			Conditional Statements
2.2.1	Conditional	$p \rightarrow q$	If p and q are statement variables, the **conditional** of q by p is "if p then q" or "p implies q", denoted $p \rightarrow q$. It is false when p is true and q is false; otherwise it is true. We called p the hypothesis (or antecedent) and q the conclusion (or consequent). this way of defining $p \rightarrow q$ gives us the nice intuitive property of the following statement which is the transitive rule of inference $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$. p → q q → r hence, p → r
2.2.2	Contrapositive	$p \rightarrow q \equiv \sim q \rightarrow \sim p$	The **contrapositive** of a conditional statement "if p then q" is "if $\sim q$ then $\sim p$". Symbolically, the contrapositive of $p \rightarrow q$ is $\sim q \rightarrow \sim p$.
2.2.3	Converse	$q \rightarrow p$	The **converse** of a conditional statement "if p then q" is "if q then p".

			Symbolically, the converse of $p \to q$ is $q \to p$.
2.2.4	Inverse	$\sim p \to \sim q$	The **inverse** of a conditional statement "if *p* then *q*" is "if ~*p* then ~*q*". Symbolically, the inverse of $p \to q$ is $\sim p \to \sim q$.
2.2.5	Only if	$p \to q \equiv$ $\sim q \to \sim p$	If *p* and *q* are statements, "*p* only if *q*" means "if not *q* then not *p*" Or, equivalently, "if *p* then *q*"
2.2.6	Biconditional (iff)	$p \leftrightarrow q$	Given statement variables *p* and *q*, the **biconditional** of *p* and *q* is "*p* if, and only if, *q*" and is denoted $p \leftrightarrow q$. It is true if both *p* and *q* have the same truth values and is false if *p* and q have opposite truth values. The words *if and only if* are sometimes abbreviated *iff*.
2.2.7	Necessary & Sufficient Conditions	$r \to s$	If *r* and *s* are statements, "*r* is a sufficient condition for *s*": • "if *r* then *s*"
		$\sim r \to \sim s$ $s \to r$	"*r* is a necessary condition for *s*": • "if not *r* then not *s*" (or "if *s* then *r*")
			Valid and Invalid Arguments
2.3.1	Argument		An **argument** (**argument form**) is a sequence of statements (statement forms). All statements in an argument (argument form), except for the final one, are called **premises** (or **assumptions** or **hypothesis**). The final statement (statement form) is called the **conclusion**. The symbol ∙, which is read "therefore", is normally placed just before the conclusion. To say that an argument form is **valid** means that no matter what particular statements are substituted for the statement variables in its premises, if the resulting premises are all true, then the conclusion is also true.
2.3.2	Sound and Unsound Arguments		An argument is called **sound** if, and only if, it is valid, and all its premises are true. An argument that is not sound is called **unsound**.
			Predicates and Quantified Statements
3.1.1	Predicate	Predicate symbols: P, Q Predicate Variables: P(x), Q(x, y)	A **predicate** is a sentence that contains a finite number of variables and becomes a statement when specific values are substituted for the variables. The **domain** of a predicate variable is the set of all values that may be substituted in place of the variable. • "domain of discourse", • "universe of discourse", • "universal set", or • "universe".
3.1.2	Truth Set	$\{x \in D \mid P(x)\}$	If *P*(*x*) is a predicate and *x* has domain *D*, the **truth set** is the set of all elements of *D* that make *P*(*x*) true when they are substituted for x.

			The truth set of $P(x)$ is denoted $\{x \in D \mid P(x)\}$. • In set theory, | is used to mean "such that".
3.1.3	Universal Statement	$\forall x \in D$, $Q(x)$	Let $Q(x)$ be a predicate and D the domain of x. A **universal statement** is a statement of the form "$\forall x \in D$, $Q(x)$". ▪ It is defined to be true iff $Q(x)$ is true for every x in D. ▪ It is defined to be false iff $Q(x)$ is false for at least one x in D. A value for x for which $Q(x)$ is false is called a **counterexample.**
3.1.4	Existential Statement	$\exists x \in D$ s.t. $Q(x)$	Let $Q(x)$ be a predicate and D the domain of x. An **existential statement** is a statement of the form "$\exists x \in D$ such that $Q(x)$". ▪ It is defined to be true iff $Q(x)$ is true for at least one x in D. ▪ It is defined to be false iff $Q(x)$ is false for all x in D. The symbol $\exists!$ is used to denote "there exists a unique" or "there is one and only one". • E.g. $\exists!\, x \in \mathbb{Z}^+$ such that x is even and prime.
Variants of Universal Conditional Statements			
3.2.1	Contrapositive	Consider a statement of the form: $\forall x \in D\ (P(x) \rightarrow Q(x))$. $\forall x \in D\ (\sim Q(x) \rightarrow \sim P(x))$	
	Converse	$\forall x \in D\ (Q(x) \rightarrow P(x))$	
	Inverse	$\forall x \in D\ (\sim P(x) \rightarrow \sim Q(x))$	
3.2.2	Sufficient Condition	$\forall x\ (r(x) \rightarrow s(x))$	"$\forall x$, $r(x)$ is a **sufficient condition** for $s(x)$" means "$\forall x\ (r(x) \rightarrow s(x))$". "$\forall x$, $r(x)$ **only if** $s(x)$" means "$\forall x\ (\sim s(x) \rightarrow \sim r(x))$" or, equivalently, "$\forall x\ (r(x) \rightarrow s(x))$".
	Necessary condition	$\forall x\ (s(x) \rightarrow r(x))$	"$\forall x$, $r(x)$ is a **necessary condition** for $s(x)$" means "$\forall x\ (\sim r(x) \rightarrow \sim s(x))$" or, equivalently, "$\forall x\ (s(x) \rightarrow r(x))$".
Arguments with Quantified Statements			
3.4.1	Valid argument form		Valid argument form: No matter what particular predicates are substituted for the predicate symbols in its premises, if the resulting premise statements are all true, then the conclusion is also true. An **argument is called valid** if, and only if, its form is valid
Sets			
5.1.1	Set		(1) A set is an unordered collection of objects (2) These objects are called the members or elements of the set. (3) Write a. $x \in A$ for x is an element of A; b. $x \notin A$ for x is not an element of A; c. $x, y \in A$ for x, y are elements of A; d. $x, y \notin A$ for x, y are not elements of A;

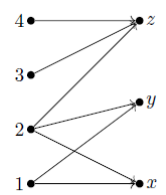
5.1.3	Roster Notation	$\{x1, x2, \ldots, xn\}$.	(1) The set whose only elements are x1, x2, . . . , xn is denoted $\{x1, x2, \ldots, xn\}$.
5.1.5	Set-builder Notation	$\{x \in U : P(x)\}$	Let U be a set and P(x) is a predicate over U. Then the set of all elements $x \in U$ such that P(x) is true is denoted $\{x \in U : P(x)\}$. • read as "the set of all x in U such that P(x)". • Some write $\{\ldots \mid \ldots\}$ for $\{\ldots : \ldots\}$. • $\{y^2 : y \text{ is an odd integer}\}$: the set of all objects of the form y^2 such that y is an odd integer • $\{t(y1, y2, \ldots, yn) : P(y1, y2, \ldots, yn)\}$ to denote $\{x : \exists y1, y2, \ldots, yn\ P(y1, y2, \ldots, yn) \wedge x = t(y1, y2, \ldots, yn)\}$
5.1.9	Equal sets	=	Two sets are equal if they have the same elements, i.e., for all sets A, B • $A = B \Leftrightarrow \forall z\, (z \in A \Leftrightarrow z \in B)$
5.1.15	Empty Set	$\varnothing$	The set with no element is called the empty set. It is denoted by $\varnothing$.
5.1.16	Subset	$\subseteq$	Let A, B be sets. Call A a subset of B, and write $A \subseteq B$, if $\forall z\, (z \in A \Rightarrow z \in B)$. • Alternatively, we may say that B includes A, and write $B \supseteq A$ in this case.
5.1.19	Proper Subset	$\subsetneq$	Let A, B be sets. Call A a proper subset of B, and write $A \subsetneq B$, if $A \subseteq B$ and A 6= B. In this case, we may say that the inclusion of A in B is proper or strict.
		Power and Products of Sets	
5.2.1	Power Set	$\mathcal{P}(A)$, $\wp(A)$	Let A be a set. The set of all subsets of A, denoted $\mathcal{P}(A)$, is called the power set of A.
5.2.3	Cardinality	$\lvert A\rvert$	(1) A set is finite if it has finitely many (distinct) elements. It is infinite if it is not finite. (2) Let A be a finite set. The cardinality of A, or the size of A, is the number of (distinct) elements in A. It is denoted by $\lvert A\rvert$. (3) Sets of size 1 are called singletons.
5.2.6	Ordered Pair	(x, y)	An ordered pair is an expression of the form (x, y). Let (x, y) and (x', y') be ordered pairs. Then • $(x, y) = (x', y') \Leftrightarrow x = x' \text{ and } y = y'$
5.2.8	Cartesian Product	$A \times B$ (A cross B)	Let A, B be sets. The Cartesian product of A and B, denoted $A \times B$, is defined to be • $\{(x, y) : x \in A \text{ and } y \in B\}$. • $\{a, b\} \times \{1, 2, 3\} = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$. • $\lvert\{a, b\} \times \{1, 2, 3\}\rvert = 6 = 2 \times 3 = \lvert\{a, b\}\rvert \times \lvert\{1, 2, 3\}\rvert$.
5.2.11	Ordered n-tuple	$(x1, x2, \ldots, xn)$.	Let $n \in \{x \in \mathbb{Z} : x > 2\}$. An ordered n-tuple is an expression of the form $(x1, x2, \ldots, xn)$. • Let $(x1, x2, \ldots, xn)$ and $(x'1, x'2, \ldots, x'n)$ be ordered n-tuples. • Then $(x1, x2, \ldots, xn) = (x'1, x'2, \ldots, x'n) \Leftrightarrow x1 = x'1$ and $x2 = x'2$ and . . . and $xn = x'n$ • (1, 2, 5) 6= (2, 1, 5), although $\{1, 2, 5\} = \{2, 1, 5\}$.
5.2.13	Cartesian Product of many sets		Let $n \in \{x \in \mathbb{Z} : x > 2\}$ and $A1, A2, \ldots, An$ be sets. The Cartesian product of $A1, A2, \ldots, An$, denoted $A1 \times A2 \times \cdots \times An$, is defined to be

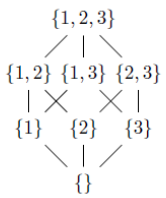
			• {(x1, x2, . . . , xn) : x1 ∈ A1 and x2 ∈ A2 and . . . and xn ∈ An} If A is a set, then $A^n = \underbrace{A \times A \times \cdots \times A}_{n\text{-many } A\text{'s}}$.
		Boolean Operations	
5.3.1	Union, Intersection, Complement	∪ (union) ∩ (intersect) \ (minus)	(1) The union of A and B, denoted A ∪ B, is defined by A ∪ B = {x : x ∈ A or x ∈ B}. (2) The intersection of A and B, denoted A ∩ B, is defined by A ∩ B = {x : x ∈ A and x ∈ B}. (3) The complement of B in A, denoted A − B or A \ B, is defined by A \ B = {x : x ∈ A and x 6∈ B}.
5.3.3	Complement	$\overline{B} = U \setminus B.$	Let B be a set. In a context where U is the universal set (so that implicitly U ⊇ B), the complement of B, denoted $\overline{B}$ or B^c, is defined by $\overline{B} = U \setminus B.$
5.3.9	Disjoint Sets		(1) Two sets A, B are disjoint if A ∩ B = ∅. (2) Sets A1, A2, . . . , An are pairwise disjoint or mutually disjoint if Ai ∩ Aj = ∅ for all distinct i, j ∈ {1, 2, . . . , n}.
		Functions	
6.1.1	Function		Let A, B be sets. A function or a map from A to B is an assignment to each element of A exactly one element of B. • f : A → B means "f is a function from A to B". • Suppose f : A → B. (1) Let x ∈ A. Then f(x) denotes the element of B that f assigns x to. If y = f(x), then we say that f maps x to y, and we may write f : x |→ y. (2) A is called the domain of f, and B is called the codomain of f. (3) The range or the image of f is {f(x) : x ∈ A} = {y ∈ B : y = f(x) for some x ∈ A}. $f : \mathbb{Z} \to \mathbb{Z};$ $x \mapsto x^3 + 23x.$ Then f is the function with domain $\mathbb{Z}$ and codomain $\mathbb{Z}$ that assigns to each $x_0 \in \mathbb{Z}$ the value of ${x_0}^3 + 23x_0$. Thus $f(0) = 0^3 + 23 \times 0 = 0$ and $f(1) = 1^3 + 23 \times 1 = 24$. The range of f is $\{x^3 + 23x : x \in \mathbb{Z}\}.$
6.1.4	Identity Function	Id_A : A → A x |→ x	Let A be a set. Then the identity function on A is the function. • The domain, the codomain, and the range of idA are all A.
6.1.6	Absolute Value	|x|	Let absval: Q → Q satisfying, for every x ∈ Q, $\text{absval}(x) = \begin{cases} x, & \text{if } x \geqslant 0; \\ -x, & \text{otherwise.} \end{cases}$ • the function absval has domain Q, codomain Q, and $\forall x \in \mathbb{Q} \;\; ((x \geqslant 0 \Rightarrow \text{absval}(x) = x) \wedge (\sim(x \geqslant 0) \Rightarrow \text{absval}(x) = -x)).$
6.1.9	Floor, ceil: Q → Z	$\lfloor x \rfloor$ and $\lceil x \rceil$	for each x ∈ Q, (1) floor(x) to be the largest integer y such that y <= x; and (2) ceil(x) to be the smallest integer y such that y >= x.

6.1.12	Sequence		**Definition 6.1.12.** A *sequence* is a function a whose domain is $\mathbb{Z}$, $\mathbb{Z}_{\geqslant k}$ or $\{x \in \mathbb{Z} : k \leqslant x \leqslant \ell\}$ for some $k, \ell \in \mathbb{Z}$. If a is a sequence, then we may write a_n for $a(n)$.
Terminology 6.1.18	Well-defined function		A function is well-defined if its definition ensures that every element of the domain is assigned exactly one element of the codomain. 
6.1.19	Equal Functions	f = g	Two functions f : A → B and g : C → D are equal if (1) A = C and B = D; and (2) f(x) = g(x) for all x ∈ A.
6.1.22	Composite Function	g ∘ f (composed with or circle)	Let f : A → B and g : B → C. Then g ∘ f : A → C such that for every x ∈ A, • (g ∘ f)(x) = g(f(x)) • For g ∘ f to be well-defined, the codomain of f must equal the domain of g
		Injectivity and Surjectivity	
6.2.1	Inverse		Let f : A → B. (1) If X ⊆ A, then let f(X) = {y ∈ B : y = f(x) for some x ∈ X} = {f(x) : x ∈ X} (2) If Y ⊆ B, then let f −1 (Y) = {x ∈ A : y = f(x) for some y ∈ Y }. • We call f(X) the (setwise) image of X, and f −1 (Y) the (setwise) preimage of Y under f • If f : A → B, then f(A) is the range/image of f.
6.2.5	Surjection, Injection, Bijection (bijective function)		Let f : A → B. (1) f is surjective or onto if ∀y ∈ B ∃x ∈ A (y = f(x)). (2) f is injective or one-to-one if ∀x, x′ ∈ A (f(x) = f(x′) ⇒ x = x′) (3) f is bijective if it is both surjective and injective, i.e., ∀y ∈ B ∃!x ∈ A (y = f(x)). • A function is surjective if and only if its codomain is equal to its range • A function f : A → B is not surjective if and only if ∃y ∈ B ∀x ∈ A (y =/= f(x)). • A function f : A → B is not injective if and only if ∃x, x′ ∈ A (f(x) = f(x′) ∧ x =/= x′)
6.2.13	Inverse		Let f : A → B. Then g : B → A is an inverse of f if • ∀x ∈ A ∀y ∈ B (y = f(x) ⇔ x = g(y))
6.2.17	Inverse		The inverse of a function f is denoted f −1
		Cardinality	
6.3.1	Same cardinality		(Cantor). (1) Two set A, B are said to have the same cardinality if there is a bijection A → B. (2) A set is countable if it is finite or it has the same cardinality as Z>=0.

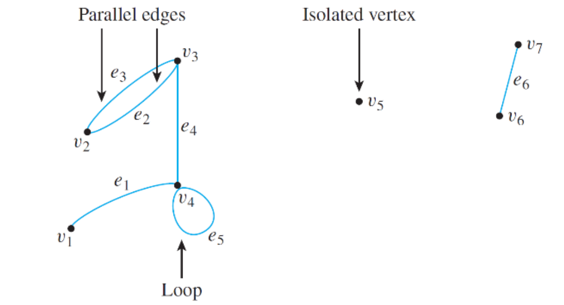
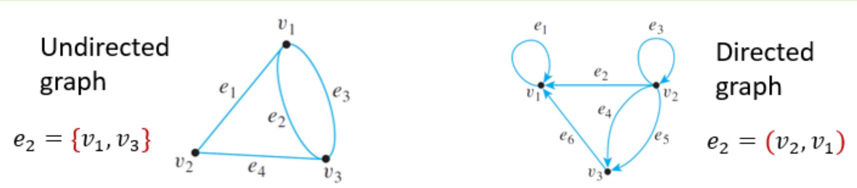
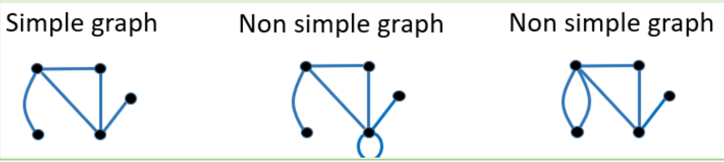
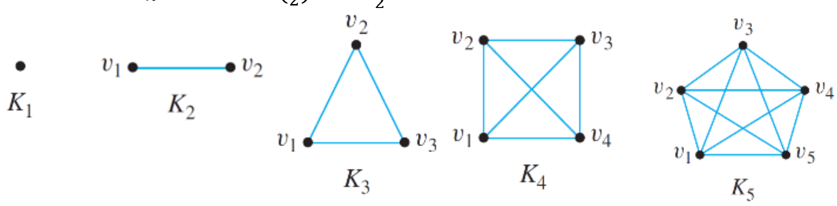
			• An infinite set B is countable if and only if there is a sequence b0, b1, b2, . . . ∈ B in which every element of B appears exactly once.
Mathematical Induction (MI)			
Principle 7.1.1	MI		Let m ∈ Z. To prove that ∀n ∈ Z>m P(n) is true, where each P(n) is a proposition, it suffices to: • (base step) show that P(m) is true • (induction step) show that ∀k ∈ Z>=m (P(k) ⇒ P(k + 1)) is true • the assumption that P(k) is true is called the induction hypothesis **Justification.** The two steps ensure the following are true: $P(m)$ by the base step; $P(m) \Rightarrow P(m+1)$ by the induction step with $k = m$; $P(m+1) \Rightarrow P(m+2)$ by the induction step with $k = m+1$; $P(m+2) \Rightarrow P(m+3)$ by the induction step with $k = m+2$; $\vdots$ We deduce that $P(m), P(m+1), P(m+2), \ldots$ are all true by a series of modus ponens.
Principle 7.2.1	Strong MI		To prove that ∀n ∈ Z>0 P(n) is true, where each P(n) is a proposition, it suffices to: • (base step) show that P(0), P(1), . . . , P(m) are true; • (induction step) show that ∀k ∈ Z>=0 (P(0) ∧ P(1) ∧ · · · ∧ P(k + m) ⇒ P(k + m + 1)) is true for some m ∈ Z>=0 **Justification.** The two steps ensure the following are true: $P(0) \wedge P(1) \wedge \cdots \wedge P(m)$ by the base step; $P(0) \wedge P(1) \wedge \cdots \wedge P(m) \Rightarrow P(m+1)$ by the induction step with $k = 0$; $P(0) \wedge P(1) \wedge \cdots \wedge P(m) \wedge P(m+1) \Rightarrow P(m+2)$ by the induction step with $k = 1$; $P(0) \wedge P(1) \wedge \cdots \wedge P(m) \wedge P(m+1) \wedge P(m+2) \Rightarrow P(m+3)$ by the induction step with $k = 2$; $\vdots$ We deduce that $P(0), P(1), P(2), P(3), \ldots$ are all true by a series of modus ponens. □
7.2.2	Fibonacci sequence		The Fibonacci sequence F0, F1, F2, . . . is defined by setting $F_0 = 0$ and $F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for each n ∈ Z>= 0.
Recursion			
Terminology 7.3.1	Recursively defined		A sequence a0, a1, a2, . . . is said to be recursively defined if the definition of an involves a0, a1, . . . , an−1 for all but finitely many n ∈ Z>=0
7.3.12	Well-Formed Formula (WFF)		Designate a nonempty set Σ whose elements will be used as propositional variables. Define the set WFF(Σ) recursively as follows (1) Every element p of Σ is in WFF(Σ). (base clause) (2) If x, y are in WFF(Σ), then $\sim x$ and $(x \wedge y)$ and $(x \vee y)$ are in WFF(Σ). (recursion clause) (3) Membership for WFF(Σ) can always be demonstrated by (finitely many) successive applications of the clauses above. (minimality clause)
7.3.16	WFF		**Definition 7.3.16.** Designate a nonempty set Σ whose elements will be used as propositional variables. Define the set WFF$^+(\Sigma)$ recursively as follows. (1) Every element p of Σ is in WFF$^+(\Sigma)$. (base clause) (2) If x, y are in WFF$^+(\Sigma)$, then $(x \wedge y)$ and $(x \vee y)$ are in WFF$^+(\Sigma)$. (recursion clause) (3) Membership for WFF$^+(\Sigma)$ can always be demonstrated by (finitely many) successive applications of the clauses above. (minimality clause)

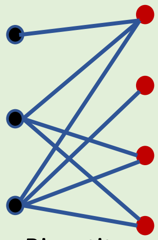
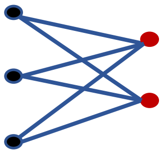
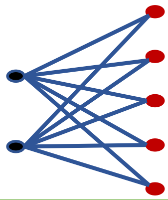
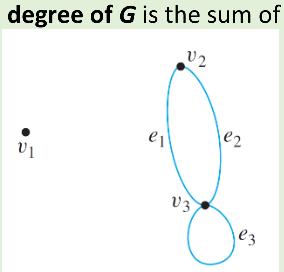
<table>
<tr><th colspan="4">Number Theory</th></tr>
<tr><th colspan="4">Divisibility</th></tr>
<tr><td>8.1.1</td><td>divides</td><td>d | n</td><td>Let n, d ∈ Z. Then d is said to divide n if n = dk for some k ∈ Z. $d \mid n$ for "d divides n", and $d \nmid n$ for "d does not divide n". "n is divisible by d" or "n is a multiple of d" or "d is a factor/divisor of n"</td></tr>
<tr><td>8.1.17</td><td>n <u>div</u> d (quotient)
n <u>mod</u> d (remainder)</td><td></td><td>Let n ∈ Z and d ∈ Z^+. The unique q, r ∈ Z given by the Division Theorem such that (n = dq + r and 0 ≤ r < d) holds are called the quotient (n div d) and the remainder (n mod d) when n is divided by d.
Remainder is always ≥ 0</td></tr>
<tr><td>8.1.21</td><td>Even and Odd integers</td><td></td><td>(1) An integer is even if it is equal to 2k for some k ∈ Z.
(2) An integer is odd if it is equal to 2k + 1 for some k ∈ Z.</td></tr>
<tr><th colspan="4">Prime Numbers</th></tr>
<tr><td>8.2.1</td><td></td><td></td><td>(1) A positive integer is prime if it has exactly two positive divisors.
(2) A positive integer is composite if it has (strictly) more than two positive divisors.
1 is neither prime nor composite because it has exactly one positive divisor.
Every integer n ≥ 2 is either prime or composite</td></tr>
<tr><th colspan="4">Base-b representation (b ≥ 2)</th></tr>
<tr><td>8.3.1</td><td>Base-b representation</td><td></td><td>Definition 8.3.1. The base-b representation of a positive integer n is $$(a_\ell a_{\ell-1} \dots a_0)_b$$ where $\ell \in \mathbb{Z}_{\geqslant 0}$ and $a_0, a_1, \dots, a_\ell \in \{0, 1, \dots, b-1\}$ such that $$n = a_\ell b^\ell + a_{\ell-1} b^{\ell-1} + \dots + a_0 b^0 \quad \text{and} \quad a_\ell \neq 0.$$ The $a_0, a_1, \dots, a_\ell$ here are called digits.</td></tr>
<tr><td>8.3.4</td><td>Names of base-b representations</td><td></td><td>(1) Base-10 representations are called decimal representations.
(2) Base-2 representations are called binary representations.
(3) Base-8 representations are called octal representations.
(4) Base-16 representations are called hexadecimal representations.
(5) Base-60 representations are called sexagesimal representations.
In hexadecimal representation, use respectively
<table><tr><td>A</td><td>B</td><td>C</td><td>D</td><td>E</td><td>F</td></tr><tr><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td></tr></table></td></tr>
<tr><th colspan="4">Greatest Common Divisors</th></tr>
<tr><td>8.4.1.</td><td>Common Divisor</td><td></td><td>Let m, n ∈ Z.
(1) A common divisor of m and n is divisor of both m and n.
(2) The greatest common divisor of m and n is denoted gcd(m, n)
Hence, $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$.</td></tr>
<tr><th colspan="4">Fundamental Theorem of Arithmetic</th></tr>
</table>

8.5.1.	Linear Combination		Let $m, n \in Z$. An integer linear combination of m and n is a number of the form $ms + nt$, where $s, t \in Z$.
8.5.7.	Prime Factorization		A prime factorization of an integer n is a way of writing n as a product of primes. e.g. $2 \times 2 \times 5 \times 5 = 2^2 5^2$
Modular Arithmetic			
8.6.1.	Congruence	≡	Let $a, b \in Z$ and $n \in Z^+$. Then a is congruent to b modulo n if $a \bmod n = b \bmod n$. In this case, we write $a \equiv b \pmod{n}$.
8.6.8.	Additive Inverse		Let $a, b \in Z$ and $n \in Z^+$. The integer b is an additive inverse of a modulo n if $a + b \equiv 0 \pmod{n}$.
8.6.15.	Multiplicative Inverse		Let $a \in Z$ and $n \in Z^+$. A multiplicative inverse of a modulo n is an integer b such that $ab \equiv 1 \pmod{n}$.
8.6.18.	Coprime		Two integers a, n are coprime if $\gcd(a, n) = 1$.
Relations			
9.1.1.	Relation		Let A, B be sets. (1) A relation from A to B is a subset of $A \times B$. (2) Let R be a relation from A to B and $(x, y) \in A \times B$. Then we may write $x \mathrel{R} y$ for $(x, y) \in R$ and $x \not\mathrel{R} y$ for $(x, y) \notin R$. e.g. Let S be the set of all NUS students and M be the set of all modules offered by the NUS. Then "is enrolled in" is a relation from S to M. As a set, this relation is $\{(x, y) \in S \times M : x \text{ is enrolled in } y\}$. e.g. Let $A = \{0, 1, 2\}$ and $B = \{1, 2, 3, 4\}$. Define the relation R from A to B by setting $x \mathrel{R} y \Leftrightarrow x < y$. Then $0 \mathrel{R} 1$ and $0 \mathrel{R} 2$, but $2 \not\mathrel{R} 1$. As a set, $R = \{(0, 1),(0, 2),(0, 3),(0, 4),(1, 2),(1, 3),(1, 4),(2, 3),(2, 4)\}$. • Those (x, y) that fulfils the requirement $(<) \in R$. **Arrow diagram.** Let $A = \{1, 2, 3, 4\}$ and $B = \{x, y, z\}$. Consider the relation R from A to B defined by $R = \{(1, x), (1, y), (2, x), (2, y), (2, z), (3, z), (4, z)\}$. One can represent this relation by the following *arrow diagram*, where the existence of an arrow from a to b indicates $a \mathrel{R} b$: 
9.2.1.	Binary Relation		A (binary) relation on a set A is a relation from A to A
9.2.2.	Reflexive, Symmetric, Transitive		Let A be a set and R be a relation on A. (1) R is reflexive if $\forall x \in A\ (x \mathrel{R} x)$. (2) R is symmetric if $\forall x, y \in A\ (x \mathrel{R} y \Rightarrow y \mathrel{R} x)$. (3) R is transitive if $\forall x, y, z \in A\ (x \mathrel{R} y \wedge y \mathrel{R} z \Rightarrow x \mathrel{R} z)$. Note: • It is wrong to say that "a is reflexive", "b is reflexive", "c is not reflexive". • We either say the relation R is reflexive or not reflexive. • We don't say an element of A is reflexive or not reflexive.

			• Reflexivity, symmetry and transitivity are properties of relations, not individual elements of A.
9.2.9.	Equivalence Relation		An equivalence relation is a relation that is reflexive, symmetric, and transitive.
9.2.10.	Equivalence Class	$[x]_R$ or simply $[x]$	Let A be a set and R be an equivalence relation on A. For each x ∈ A, the equivalence class of x with respect to R, denoted $[x]_R$, is defined by $[x]_R = \{y \in A: x \mathrel{R} y\}$. • Define $A/R = \{[x]_R: x \in A\}$. **Example 9.2.12.** Fix $n \in \mathbb{Z}^+$. The congruence-mod-n relation R_n on $\mathbb{Z}$ is an equivalence relation. The equivalence classes are of the form $[x] = \{y \in \mathbb{Z} : x \equiv y \pmod n\} = \{x + nk : k \in \mathbb{Z}\},$ where $x \in \mathbb{Z}$. So $\mathbb{Z}/R_n = \{\{x + nk : k \in \mathbb{Z}\} : x \in \mathbb{Z}\} = \{[0], [1], \ldots, [n-1]\}$. If $n = 2$, then there are two equivalence classes: $\{2k : k \in \mathbb{Z}\}$ and $\{2k + 1 : k \in \mathbb{Z}\}$.
Partitions			
9.3.1.	Partition	C	A partition of a set A is a set C of nonempty subsets of A such that (≥ 1) ∀x ∈ A ∃S ∈ C (x ∈ S); and (≤ 1) ∀x ∈ A ∀S, S' ∈ C (x ∈ S ∧ x ∈ S' ⇒ S = S') Elements of a partition are called components of the partition. e.g. The set A = {1, 2, 3} has the following partitions: • {{1}, {2}, {3}}, • {{1}, {2, 3}}, • {{2}, {1, 3}}, • {{3}, {1, 2}}, • {{1, 2, 3}} e.g. The congruence-mod-2 relation gives rise to the following partition of Z • {{2k : k ∈ Z}, {2k + 1 : k ∈ Z}}
Partial Orders			
9.4.1.	Partial Order	$\preceq$ $\prec$ (for $x \preceq y \wedge x \neq y$.)	Let A be a set and R be a relation on A. (1) R is antisymmetric if ∀x, y ∈ A (x R y ∧ y R x ⇒ x = y). (2) R is a (non-strict) partial order if R is reflexive, antisymmetric, and transitive. (3) Suppose R is a partial order. Let x, y ∈ A. Then x, y are comparable (under R) if x R y or y R x. (4) R is a (non-strict) total order if R is a partial order and ∀x, y ∈ A (x R y ∨ y R x). (connex) <u>Note 9.4.2.</u> A total order is always a partial order <u>Note:</u> "divides" relation on integers is a partial order
9.4.11.	Hasse Diagram		Let $\preceq$ be a partial order on a set A. A Hasse diagram of $\preceq$ satisfies the following condition for all x, y ∈ A • If $x \prec y$ and no z ∈ A is such that $x \prec z \prec y$, then x is placed below y and there is a line joining x to y, else no line joins x to y. **Example 9.4.13.** Consider $\mathcal{P}(\{1, 2, 3\})$ partially ordered by the inclusion relation $\subseteq$. A Hasse diagram is as follows: 
Linearisation			

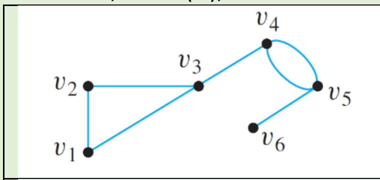
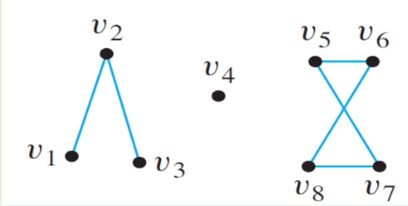
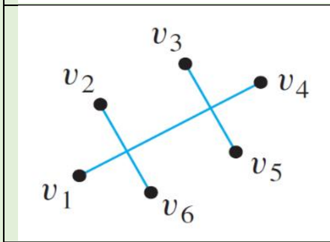
9.5.1.	Minimal, Maximal, smallest, largest		Let $\preceq$ be a partial order on a set A. (1) c is a minimal element if $\forall x \in A\ (x \preceq c \Rightarrow c = x)$. (2) c is a maximal element if $\forall x \in A\ (c \preceq x \Rightarrow c = x)$. (3) c is the smallest element (or the minimum element) if $\forall x \in A\ (c \preceq x)$. (4) c is the largest element (or the maximum element) if $\forall x \in A\ (x \preceq c)$.
9.5.4.	Well-order		A well-order on a set A is a total order on A with respect to which every nonempty subset of A has a smallest element.
Tut 8	Inverse relation	R^{-1}	Let R be a relation from a set A to a set B. R^{-1} is the inverse relation of R, i.e. $$R^{-1} = \{(y, x) : (x, y) \in R\}, \text{ or}$$ $$y\, R^{-1}\, x \Leftrightarrow x\, R\, y$$ for each $y \in B$ and each $x \in A$.
Counting			
Sample Space			A **sample space** is the set of all possible outcomes of a random process or experiment.
Event			An event is a subset of a sample space.
No. of elements		$\|A\|$	For a finite set A, $\|A\|$ denotes the number of elements in A.
r-permutation		$P(n, r)$	An ***r*-permutation** of a set of n elements is an ordered selection of r elements taken from the set.
r-combination		$\binom{n}{r}$	Let n and r be non-negative integers with $r \leq n$. An ***r*-combination** of a set of n elements is a subset of r of the n elements. $\binom{n}{r}$, read "n choose r", denotes the number of subsets of size r (r-combinations) that can be chosen from a set of n elements. Other symbols used are $C(n, r)$, ${}_nC_r$, $C_{n,r}$, or ${}^nC_r$.
Multiset			An ***r*-combination with repetition allowed**, or **multiset of size *r***, chosen from a set X of n elements is an unordered selection of elements taken from X with repetition allowed. If $X = \{x_1, x_2, \cdots, x_n\}$, we write an r-combination with repetition allowed as $[x_{i_1}, x_{i_2}, \cdots, x_{i_r}]$ where each x_{i_j} is in X and some of the x_{i_j} may equal each other.
Expected Value			Suppose the possible outcomes of an experiment, or random process, are real numbers $a_1, a_2, a_3, \cdots, a_n$ which occur with probabilities $p_1, p_2, p_3, \cdots, p_n$. The **expected value** of the process is $$\sum_{k=1}^{n} a_k p_k = a_1 p_1 + a_2 p_2 + a_3 p_3 + \cdots + a_n p_n$$
Linearity of Expectation			The expected value of the sum of random variables is equal to the sum of their individual expected values, regardless of whether they are independent. For random variables X and Y, $$E[X + Y] = E[X] + E[Y]$$ For random variables $X_1, X_2, \cdots, X_n$ and constants $c_1, c_2, \cdots, c_n$, $$E\left[\sum_{i=1}^{n} c_i \cdot X_i\right] = \sum_{i=1}^{n} (c_i \cdot E[X_i])$$
Conditional Probability			Let A and B be events in a sample space S. If $P(A) \neq 0$, then the **conditional probability of *B* given *A***, denoted $P(B\|A)$, is $$P(B\|A) = \frac{P(A \cap B)}{P(A)}$$ $$P(A \cap B) = P(B\|A) \cdot P(A)$$ $$P(A) = \frac{P(A \cap B)}{P(B\|A)}$$
Independent Events			If A and B are events in a sample space S, then A and B are **independent**, if and only if, $P(A \cap B) = P(A) \cdot P(B)$

Pairwise Independent and Mutually Independent		Let A, B and C be events in a sample space S. A, B and C are **pairwise independent**, if and only if, they satisfy conditions 1 – 3 below. They are **mutually independent** if, and only if, they satisfy all four conditions below. 1. $P(A \cap B) = P(A) \cdot P(B)$ 2. $P(A \cap C) = P(A) \cdot P(C)$ 3. $P(B \cap C) = P(B) \cdot P(C)$ 4. $P(A \cap B \cap C) = P(A) \cdot P(B) \cdot P(C)$
Graphs		
Edge		• An edge is said to **connect** its endpoints; • An edge is said to be **incident on** each of its endpoints, and • two edges incident on the same endpoint are called **adjacent edges**.  • $e_1 = \{v_1, v_4\}$; • $e_2 = e_3 = \{v_2, v_3\}$; • $e_4 = \{v_3, v_4\}$; • $e_5 = \{v_4, v_4\}$; • $e_6 = \{v_6, v_7\}$.
Adjacent vertices		two vertices that are connected by an edge are called **adjacent vertices**; and
Loop		a vertex that is an endpoint of a loop is said to be **adjacent to itself**.
Undirected graph	$e = \{v, w\}$	An undirected **graph** G consists of 2 finite sets: a nonempty set V of **vertices** and a set E of **edges**, where each (undirected) edge is associated with a set consisting of either one or two vertices called its **endpoints**. • We write $e = \{v, w\}$ for an undirected edge e incident on vertices v and w. 
Directed graph	$e = (v, w)$	A **directed graph**, or **digraph**, G, consists of 2 finite sets: a nonempty set V of **vertices** and a set E of **directed edges**, where each (directed) edge is associated with an **ordered pair** of vertices called its **endpoints**. • We write $e = (v, w)$ for a directed edge e from vertex v to vertex w.
Simple graph		A **simple graph** is an undirected graph that does <u>not</u> have any loops or parallel edges. • That is, there is at most one edge between each pair of distinct vertices. 
Complete graph		A **complete graph** on ***n* vertices**, $n > 0$, denoted $\boldsymbol{K_n}$, is a simple graph with n vertices and exactly one edge connecting each pair of distinct vertices. (tut 11 Q5) A K_n graph has $\binom{n}{2} = \frac{n(n-1)}{2}$ edges. 

Bipartite graph		A **bipartite graph** (or bigraph) is a simple graph whose vertices can be divided into two disjoint sets U and V such that every edge connects a vertex in U to one in V.  Bipartite
Complete Bipartite graph		A **complete bipartite graph** is a bipartite graph on two disjoint sets U and V such that every vertex in U connects to every vertex in V. If $\|U\| = m$ and $\|V\| = n$, the complete bipartite graph is denoted as $K_{m,n}$.  $K_{3,2}$  $K_{2,5}$
Subgraph of a graph		A graph *H* is said to be a **subgraph** of graph *G* iff every vertex in *H* is also a vertex in *H*, 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 graph and *v* a vertex of *G*. The **degree** of *v*, denoted **deg(*v*)**, equals the number of edges that are incident on *v*, with an edge that is a loop counted twice.
Total degree of a graph		The **total degree of *G*** is the sum of the degrees of all the vertices of *G*.  • deg(v_1) = 0 • deg(v_2) = 2 • deg(v_3) = 4 • Total degree of *G* = 6
Walk	$v_0\, e_1\, v_1\, e_2 \ldots v_{n-1}\, e_n\, v_n$	Let *G* be a graph, and let *v* and *w* be vertices of *G*. A **walk from *v* to *w*** is a finite alternating sequence of adjacent vertices and edges of *G*. Thus a walk has the form $v_0\, e_1\, v_1\, e_2 \ldots v_{n-1}\, e_n\, v_n$, where the *v*'s represent vertices, the *e*'s represent edges, $v_0=v$, $v_n=w$, and for all $i \in \{1, 2, \ldots, n\}$, v_{i-1} and v_i are the endpoints of e_i. • The number of edges, *n*, is the **length** of the walk. • The **trivial walk** from *v* to *v* consists of the single vertex *v*.
Trail		A **trail from *v* to *w*** is a walk from *v* to *w* that does not contain a repeated edge.
Path		A **path from *v* to *w*** is a trail that does not contain a repeated vertex.
Closed walk		A **closed walk** is a walk that starts and ends at the same vertex.
Circuit (aka cycle)		Let $n \in \mathbb{Z}_{\geq 3}$. An undirected graph $G(V, E)$ where $V = \{x_1, x_2, \cdots, x_n\}$ and $E = \{\{x_1, x_2\}, \{x_2, x_3\}, \cdots, \{x_{n-1}, x_n\}, \{x_n, x_1\}\}$ is called **a circuit/cycle**.
Simple circuit		A **simple circuit** (or **simple cycle**) is a circuit that does not have any other repeated vertex except the first and last.
Cyclic graph		An undirected graph is **cyclic** if it contains a loop or a cycle; otherwise, it is **acyclic.**
Connectedness		• **Two vertices** *v* and *w* of a graph *G* are **connected** iff there is a walk from *v* to *w*.

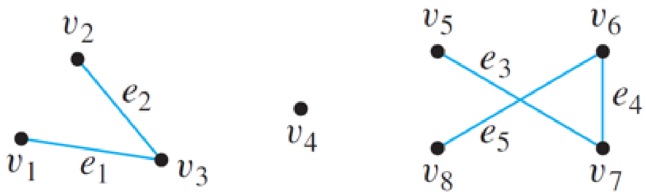
<table>
<tr><td></td><td></td><td>

- **The graph *G* is connected** iff given *any* two vertices *v* and *w* in *G*, there is a walk from *v* to *w*. Symbolically, *G* is connected iff ∀ vertices *v*, *w* ∈ *V*(*G*), ∃ a walk from *v* to *w*.

<table>
<tr><td>
</td><td>Connected</td></tr>
<tr><td>
</td><td>Not connected</td></tr>
<tr><td>
</td><td>Not connected</td></tr>
</table>
</td></tr>
<tr><td>Connected component</td><td></td><td>

A graph *H* is a **connected component** of a graph *G* iff

1. The graph *H* is a subgraph of *G*;
2. The graph *H* is connected; and
3. No connected subgraph of *G* has *H* as a subgraph and contains vertices or edges that are not in *H*.



G has 3 connected components H_1, H_2 and H_3 with vertex sets V_1, V_2 and V_3 and edge sets E_1, E_2 and E_3 , where

$V_1 = \{v_1, v_2, v_3\}$ $E_1 = \{e_1, e_2\}$

$V_2 = \{v_4\}$ $E_2 = \emptyset$

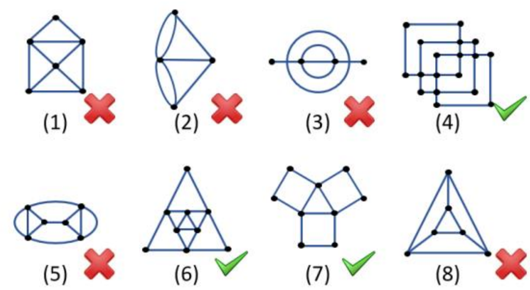
$V_3 = \{v_5, v_6, v_7, v_8\}$ $E_3 = \{e_3, e_4, e_5\}$
</td></tr>
<tr><td>Euler circuit</td><td></td><td>

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

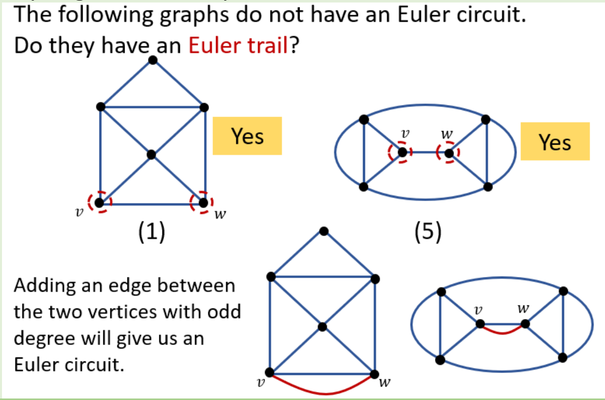
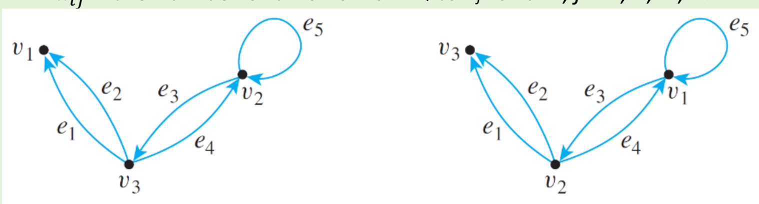
- (Thm 10.2.4.) A graph *G* has an Euler circuit iff *G* is connected and every vertex of *G* has positive even degree.
</td></tr>
<tr><td>Euler graph</td><td></td><td>

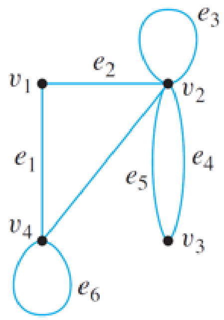
An **Eulerian graph** is a graph that contains an Euler circuit.

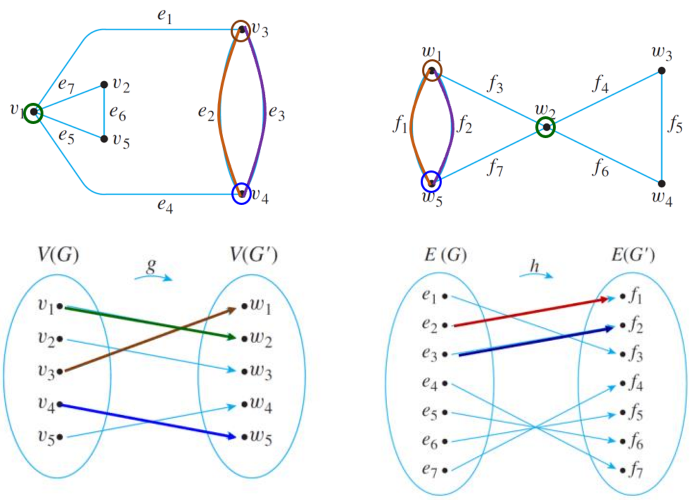
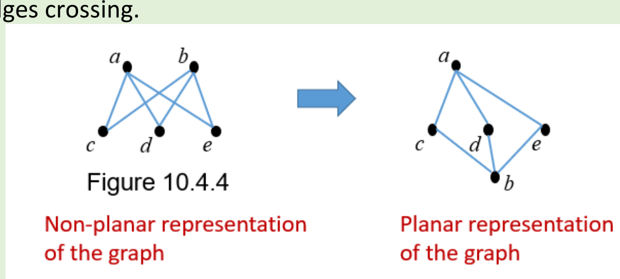
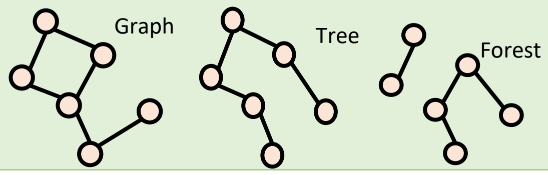
Does each of the following graphs have an Euler circuit?

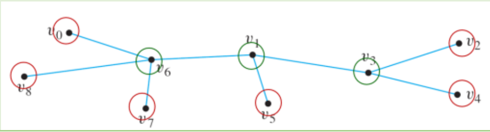
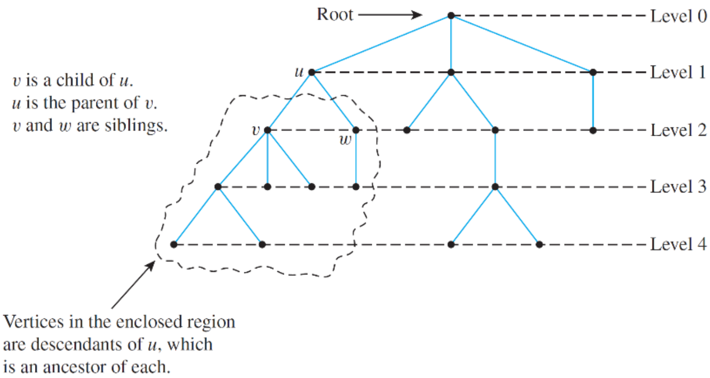


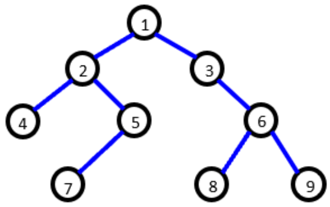
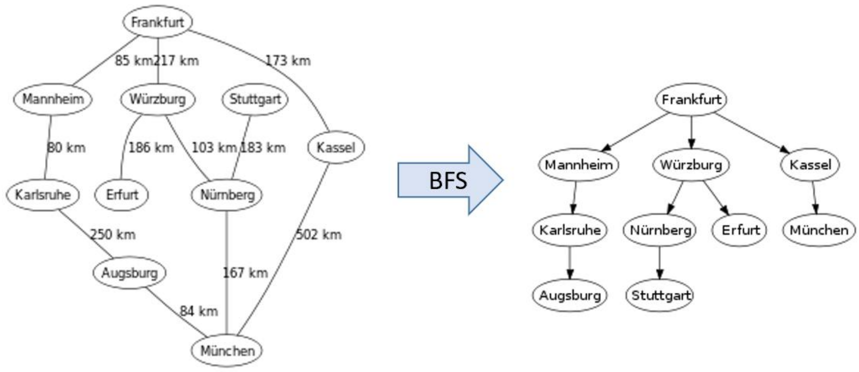
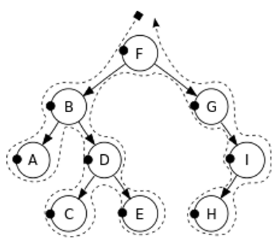
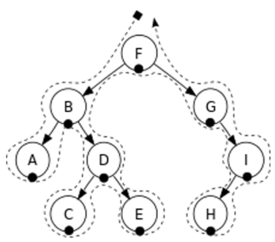
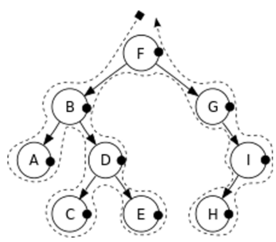
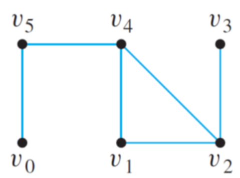
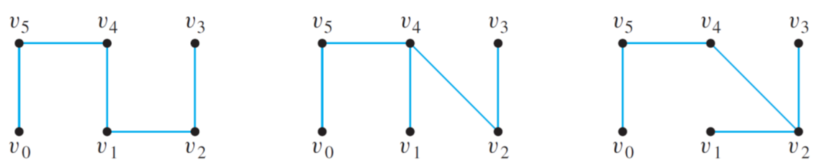
</td></tr>
<tr><td>Euler trail</td><td></td><td>Let *G* be a graph, and let *v* and *w* be two distinct vertices of *G*.</td></tr>
</table>

		An **Euler trail/path from *v* to *w*** is a sequence of adjacent edges and vertices that starts at *v*, ends at *w*, passes through every vertex of *G* at least once, and traverses every edge of *G* exactly once. 
Hamiltonian Circuit		Given a graph *G*, a **Hamiltonian circuit** for *G* is a simple circuit that includes every vertex of *G*. • That is, every vertex appears exactly once, except for the first and the last, which are the same.
Hamiltonian Graph (aka **Hamilton graph**)		A **Hamiltonian graph** is a graph that contains a Hamiltonian circuit. (Prop 10.2.6.) If a graph *G* has a Hamiltonian circuit, then *G* has a subgraph *H* with the following properties: 1. *H* contains every vertex of *G*. 2. *H* is connected. 3. *H* has the same number of edges as vertices. 4. Every vertex of *H* has degree 2.
Matrix		An $m \times n$ (read "*m* by *n*") **matrix** A over a set *S* is a rectangular array of elements of *S* arranged into *m* rows and *n* columns. $\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1j} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2j} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{ij} & \cdots & a_{in} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mj} & \cdots & a_{mn} \end{bmatrix}$ ← ith row of **A** jth column of **A**
Adjacency matrix of a directed graph		Let *G* be a directed graph with ordered vertices $v_1, v_2, \ldots v_n$. The **adjacency matrix of *G*** is the $n \times n$ matrix $\mathbf{A} = (a_{ij})$ over the set of non-negative integers such that a_{ij} = the number of arrows from v_i to v_j for all $i, j = 1, 2, \ldots, n$.  $\begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \end{array}\begin{array}{c} \begin{array}{ccc} v_1 & v_2 & v_3 \end{array} \\ \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 2 & 1 & 0 \end{bmatrix} \end{array}$ $\qquad$ $\begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \end{array}\begin{array}{c} \begin{array}{ccc} v_1 & v_2 & v_3 \end{array} \\ \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 2 \\ 0 & 0 & 0 \end{bmatrix} \end{array}$
Adjacency Matrix of an Undirected Graph		Let *G* be an undirected graph with ordered vertices $v_1, v_2, \ldots v_n$. The **adjacency matrix of *G*** is the $n \times n$ matrix $\mathbf{A} = (a_{ij})$ over the set of non-negative integers such that a_{ij} = the number of edges connecting v_i and v_j for all $i, j = 1, 2, \ldots, n$.

		 $\mathbf{A} = \begin{array}{c c} & \begin{array}{cccc} v_1 & v_2 & v_3 & v_4 \end{array} \\ \begin{array}{c} v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} & \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 2 & 1 \\ 0 & 2 & 0 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix} \end{array}$ Note that the matrix is symmetric.
Symmetric matrix		An $n \times n$ square matrix A = (a_{ij}) is called **symmetric** if, and only if, $a_{ij} = a_{ji}$ for all *i*, *j* = 1, 2, ..., *n*.
Scalar product of matrix		Suppose that all entries in matrices **A** and **B** are real numbers. If the number of elements, *n*, in the *i*th row of **A** equals the number of elements in the *j*th column of **B**, then the **scalar product** or **dot product** of the *i*th row of **A** and the *j*th column of **B** is the real number obtained as follows: $$[a_{i1} \quad a_{i2} \quad \cdots \quad a_{in}] \begin{bmatrix} b_{1j} \\ b_{2j} \\ \vdots \\ b_{nj} \end{bmatrix} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj}$$
Matrix multiplication		Let **A** = (a_{ij}) be an $m \times k$ matrix and **B** = (b_{ij}) an $k \times n$ matrix with real entries. The (matrix) product of **A** times **B**, denoted **AB**, is that matrix (c_{ij}) defined as follows: $$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1k} \\ a_{21} & a_{22} & \cdots & a_{2k} \\ \vdots & \vdots & & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{ik} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mk} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1j} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2j} & \cdots & b_{2n} \\ & \cdot & & \cdot & & \cdot \\ & \cdot & & \cdot & & \cdot \\ & \cdot & & \cdot & & \cdot \\ b_{k1} & b_{k2} & \cdots & b_{kj} & \cdots & b_{kn} \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1j} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2j} & \cdots & c_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ c_{i1} & c_{i2} & \cdots & \boxed{c_{ij}} & \cdots & c_{in} \\ \vdots & \vdots & & \vdots & & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mj} & \cdots & c_{mn} \end{bmatrix}$$ where $c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{ik}b_{kj} = \sum_{r=1}^{k} a_{ir}b_{rj}$. for all *i* = 1, 2, ..., *m* and *j* = 1, 2, ..., *n*. $$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ 0 & 1 \end{bmatrix}, \quad \text{but} \quad \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}.$$ • Multiplication of real numbers is commutative, but matrix multiplication is not. • both real number and matrix multiplications are associative ((*ab*)*c* = *a*(*bc*)
Identity matrix		For each positive integer *n*, the ***n* × *n* identity matrix**, denoted $I_n = (\delta_{ij})$ or just **I** (if the size of the matrix is obvious from context), is the *n* × *n* matrix in which all the entries in the main diagonal are 1's and all other entries are 0's. In other words, $$\delta_{ij} = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases} \; for\ all\ i, j = 1,\ 2,\ \ldots,\ n$$ $$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix} = \begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix}$$ $$\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$$
n^{th} Power of a Matrix		For any *n* × *n* matrix **A**, the **powers of A** are defined as follows: $\mathbf{A}^0 = \mathbf{I}$ where **I** is the *n* × *n* identity matrix $\mathbf{A}^n = \mathbf{A}\,\mathbf{A}^{n-1}$ for all integers $n \geq 1$
Isomorphic Graph		Let $G = (V_G, E_G)$ and $G' = (V_{G'}, E_{G'})$ be two graphs. ***G* is isomorphic to *G′***, denoted $G \cong G'$, if and only if there exist bijections $g: V_G \to V_{G'}$ and $h: E_G \to E_{G'}$ that preserve the edge-endpoint functions of G and G' in the sense that for all $v \in V_G$ and $e \in E_G$, v is an endpoint of $e \Leftrightarrow g(v)$ is an endpoint of $h(e)$.

		<u>Alternative definition:</u> **G is isomorphic to G'** if and only if there exists a permutation $\pi: V_G \rightarrow V_{G'}$ such that $\{u, v\} \in E_G \Leftrightarrow \{\pi(u), \pi(v)\} \in E_{G'}$. Show that the following two graphs are isomorphic. 
Planar graph		A **planar graph** is a graph that can be drawn on a (two-dimensional) plane without edges crossing. 
Complement graph (tut 11)		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. The figure below shows a graph G and its complement $\bar{G}$.  A graph G and its complement $\bar{G}$.
Self-complementary graph (tut 11)		A self-complementary graph is isomorphic with its complement.
Triangle (tut 11)		A simple circuit (cycle) of length three is called a triangle.
Trees (The graph is assumed to be undirected here)		
Circuit-free		A **graph** is said to be **circuit-free** if and only if it has no circuits.
Tree		A graph is called a **tree** if and only if it is circuit-free and connected. • A **trivial tree** is a graph that consists of a single vertex. 
Forest		A graph is called a **forest** if and only if it is circuit-free and not connected. (tut 11 Q6) a forest with v vertices and k components has (v - k) edges.

Terminal vertex (leaf) and internal vertex		Let *T* be a tree. • If *T* has only one or two vertices, then each is called a **terminal vertex** (or **leaf**). • If *T* has at least three vertices, then a vertex of degree 1 in *T* is called a **terminal vertex** (or **leaf**), and a vertex of degree greater than 1 in *T* is called an **internal vertex**.  <u>Leaves:</u> v_0, v_2, v_4, v_5, v_7 & v_8. <u>Internal vertices:</u> v_6, v_1 & v_3.
Rooted tree		A **rooted tree** is a tree in which there is one vertex that is distinguished from the others and is called the **root**.
Level		The **level** of a vertex is the number of edges along the unique path between it and the root.
Height		The **height** of a rooted tree is the maximum level of any vertex of the tree.
Child		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*.
Parent		If *w* is a child of *v*, then *v* is called the **parent** of *w*.
Siblings		Two distinct vertices that are both children of the same parent are called **siblings**.
Ancestor, descendant		Given two distinct vertices *v* and *w*, if *v* lies on the unique path between *w* and the root, then *v* is an **ancestor** of *w*, and *w* is a **descendant** of *v*. 
Binary tree		A **binary tree** is a rooted tree in which every parent has at most two children. Each child is designated either a **left child** or a **right child** (but not both), and every parent has at most one left child and one right child.
Full binary tree		A **full binary tree** is a binary tree in which each parent has exactly two children.
Left/Right subtree		Given any parent *v* in a binary tree *T*, if *v* has a left child, then the **left subtree** of *v* is the binary tree whose root is the left child of *v*, whose vertices consist of the left child of *v* and all its descendants, and whose edges consist of all those edges of *T* that connect the vertices of the left subtree. The **right subtree** of *v* is defined analogously.
Breadth-First Search		In breadth-first search (by E.F. Moore), it starts at the root and visits its adjacent vertices, and then moves to the next level.

		 
Depth-First Search	**Pre-order**	▪ Print the data of the root (or current vertex) ▪ Traverse the left subtree by recursively calling the pre-order function ▪ Traverse the right subtree by recursively calling the pre-order function
	In-order	▪ Traverse the left subtree by recursively calling the in-order function ▪ Print the data of the root (or current vertex) ▪ Traverse the right subtree by recursively calling the in-order function
	Post-order	▪ Traverse the left subtree by recursively calling the post-order function ▪ Traverse the right subtree by recursively calling the post-order function ▪ Print the data of the root (or current vertex)
	 Pre-order: F, B, A, D, C, E, G, I, H	 In-order: A, B, C, D, E, F, G, H, I  Post-order: A, C, E, D, B, H, I, G, F
Spanning tree		A **spanning tree** for a graph *G* is a subgraph of *G* that contains every vertex of *G* and is a tree. (tut 11 Q8) The number of spanning trees in a complete graph K_n is n^{n-2}. Find all spanning trees for the graph *G* below.  The graph *G* has one circuit $v_2v_1v_4v_2$ and removal of any edge of the circuit gives a tree. Hence there are three spanning trees for *G*. 

Weighted graph		A **weighted graph** is a graph for which each edge has an associated positive real number **weight** . The sum of the weights of all the edges is the **total weight** of the graph. • If G is a weighted graph and e is an edge of G, then $\boldsymbol{w(e)}$ denotes the weight of e and $\boldsymbol{w(G)}$ denotes the total weight of G.
Minimum spanning tree		A **minimum spanning tree** for a connected weighted graph is a spanning tree that has the least possible total weight compared to all other spanning trees for the graph.

Theorem	
Logic of Quantified Statement	
Tut 1 Q9	The product of any two odd integers is an odd integer.
Tut 1 Q10	If a,b,c are integers such that $a^2+b^2=c^2$, then a,b cannot both be odd
Tut 2 Q3	$\forall a,b,c \in \mathbb{Z}$, if $a-b$ is even and $a-c$ is even, then $b-c$ is even
Assignment 1 Q7	Let a be a rational number and b an irrational number. $\boldsymbol{a \neq 0 \rightarrow ab}$ is irrational.
Assignment 1 Q8	$\forall\ \boldsymbol{n} \in \mathbb{Z}\ \ \boldsymbol{n}^2 + \boldsymbol{n}$ is even.
Midterms Q21	T25. Suppose $a$and $b$are real numbers, if $ab > 0$, then both a and b are positive or both are negative. Prove that $\forall\ x \in \mathbb{R}\ ((x^2 > x) \rightarrow (x < 0) \vee (x > 1))$.
3.2.1	Negation of a Universal Statement: • $\sim(\forall\ x \in D,\ P(x)) \equiv \exists\ x \in D$ such that $\sim P(x)$
3.2.2	Negation of an Existential Statement: • $\sim(\exists\ x \in D$ s.t. $P(x)) \equiv \forall\ x \in D,\ \sim P(x)$
3.2.3	Negations of Universal Conditional Statements: • $\sim(\forall\ x\ (P(x) \rightarrow Q(x))) \equiv \exists\ x$ s.t. $(P(x) \wedge \sim Q(x))$
Methods of Proof	
4.3.1	Every integer is a rational number.
4.3.2	The sum of any two rational numbers is rational.
Corollary 4.2.3	The double of a rational number is rational. (special case of Theorem 4.3.2)
4.4.1	For all positive integers a and b, if $a \mid b$, then $a \leq b$.
4.4.2	The only divisors of 1 are 1 and -1
4.4.3	For all integers a, b and c, if $a \mid b$ and $b \mid c$, then $a \mid c$.
4.7.1	There is no greatest integer.
4.7.4	For all integers n, if n^2 is even than n is even.
Set Theory	
5.1.14	There exists a unique set with no element, i.e. • (existence) there is a set with no element; and • (uniqueness) for all sets A, B, if both A and B have no element, then A = B.
5.2.4	Let A be a finite set. Then $\lvert \mathcal{P}(A) \rvert = 2^{\lvert A \rvert}$.
5.3.5	(Set Identities). For all set A, B, C in a context where U is the universal set, the following hold

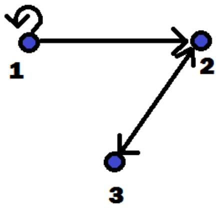
	Identity Laws: $A \cup \varnothing = A$, $A \cap U = A$ Universal Bound Laws: $A \cup U = U$, $A \cap \varnothing = \varnothing$ Idempotent Laws: $A \cup A = A$, $A \cap A = A$ Double Complement Law: $\overline{(\overline{A})} = A$ Commutative Laws: $A \cup B = B \cup A$, $A \cap B = B \cap A$ Associative Laws: $(A \cup B) \cup C = A \cup (B \cup C)$, $(A \cap B) \cap C = A \cap (B \cap C)$ Distributive Laws: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ De Morgan's Laws: $\overline{A \cup B} = \overline{A} \cap \overline{B}$, $\overline{A \cap B} = \overline{A} \cup \overline{B}$ Absorption Laws: $A \cup (A \cap B) = A$, $A \cap (A \cup B) = A$ Complement Laws: $A \cup \overline{A} = U$, $A \cap \overline{A} = \varnothing$ Set Difference Law: $A \setminus B = A \cap \overline{B}$ $\overline{\varnothing} = U$, $\overline{U} = \varnothing$ **One of De Morgan's Laws.** Work in the universal set U. For all sets A, B, $\overline{A \cup B} = \overline{A} \cap \overline{B}$.
5.3.11	(1) Let A, B be disjoint finite sets. Then |A ∪ B| = |A| + |B|. (2) Let A1, A2, . . . , An be pairwise disjoint finite sets. Then |A1 ∪ A2 ∪ · · · ∪ An| = |A1| + |A2| + · · · + |An|
5.3.12	(Inclusion–Exclusion Principle). For all finite sets A, B • |A ∪ B| = |A| + |B| − |A ∩ B|.
Tut 3 Q4	{2n+ 1 : n ∈ Z} = {2n−1 : n ∈ Z}.
Tut 3 Q9	Let A, B be sets. A⊆B ⇔ A∪B = B.
Assignment 1 Q10	Let A, B be sets. Show that if $\mathcal{P}(A \cup B) \subseteq \mathcal{P}(A) \cup \mathcal{P}(B)$, then either $A \subseteq B$ or $B \subseteq A$.
	Functions
Exercise 6.1.8.	Show that the range of absval is Q≥0.
Exercise 6.1.11.	Let x ∈ Q. (1) Show that math_floor(x) is the unique y ∈ Z such that y 6 x < y + 1. (2) Show that math_ceil(x) is the unique y ∈ Z such that y − 1 < x 6
6.1.26	Associativity of function composition: • Let f : A → B and g : B → C and h: C → D. Then (h ∘ g) ∘ f = h ∘ (g ∘ f).
Proposition 6.2.16	Uniqueness of inverses • If g, g' are inverses of f : A → B, then g = g'.
6.2.17	A function f : A → B is bijective if and only if it has an inverse.
Proposition 6.3.4	Any subset A of a countable set B is countable
Proposition 6.3.5	Every infinite set B has a countable infinite subset.
6.3.6	(Cantor 1877). Z>= 0 × Z>=0 is countable (cartesian product)
Corollary 6.3.7	Q is countable (set of rational numbers)
6.3.8	(Cantor 1891). Let A be a countable infinite set. Then $\mathcal{P}$ (A) is not countable.
Corollary 6.3.9	R is not countable
Tut 4 Q4 (a)	Let f: B → C. Suppose f is injective. Show that g ∘ f is injective whenever g is an injective function with domain C.
Tut 4 Q4 (b)	Suppose there exists a function g with domain C such that g ∘ f is injective. Show that f is injective.
Tut 4 Q5 (a)	Let f: B → C. Suppose f is surjective. Show that f ∘ h is surjective whenever h is a surjective function with codomain B.
Tut 4 Q5 (b)	Suppose we have a function h with codomain B such that f ∘ h is surjective. Show that f is surjective.

Tut 4 Q6	The order of a bijection f: A → A is defined to be the least n ∈ Z_+ such that $\underbrace{f \circ f \circ \ldots \circ f}_{n\text{-many } f\text{'s}} = \mathrm{id}_A$.
Tut 4 Q7	Let A, B, C be sets. Show that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ for all bijections f: A → B and all bijections g: B → C.
Tut 4 Q9	Let f: A → B be a function. Let X ⊆ A and Y ⊆ B. • It is always the case that $X \subseteq f^{-1}(f(X))$. • It is always the case that $f(f^{-1}(Y)) \subseteq Y$.
Midterms Q16	$\forall X \subseteq \mathbb{Z}\ \ f^{-1}(f(X)) \subseteq X$ For $f\colon \mathbb{Z} \to \mathbb{Z}$, the above condition is satisfied if f is injective.
Midterms Q17	$\forall Y \subseteq \mathbb{Z}\ \ Y \subseteq f(f^{-1}(Y))$ For $f\colon \mathbb{Z} \to \mathbb{Z}$, the above condition is satisfied if f is surjective.
	Induction
7.2.7	(Strong MI, alternative formulation). To prove that ∀n ∈ Z>0 P(n) is true, where each P(n) is a proposition, it suffices to show that $\forall \ell \in \mathbb{Z}_{\geqslant 0}\ \ (\forall i \in \mathbb{Z}_{\geqslant 0}\ \ (i < \ell \Rightarrow P(i)) \Rightarrow P(\ell))$ is true.
7.2.9	(Well-Ordering Principle). Every nonempty subset of Z ≥ 0 (or Z ≥ m for a fixed m) has a smallest element
Proposition 7.3.4	There is a unique sequence a0, a1, a2, . . . satisfying, for each n ∈ Z ≥ 0, $a_0 = 0$ and $a_1 = 1$ and $a_{n+2} = a_{n+1} + a_n$.
7.3.5	Z ≥ 0 is the unique set with the following properties ➔ recursive definition of Z>=0 (1) $0 \in \mathbb{Z}_{\geqslant 0}$. (base clause) (2) If $x \in \mathbb{Z}_{\geqslant 0}$, then $x+1 \in \mathbb{Z}_{\geqslant 0}$. (recursion clause) (3) Membership for $\mathbb{Z}_{\geqslant 0}$ can always be demonstrated by (finitely many) successive applications of the clauses above. (minimality clause)
7.3.10	**Theorem 7.3.10** (Structural induction over $2\mathbb{Z}_{\geqslant 1}$). To prove that $\forall n \in 2\mathbb{Z}_{\geqslant 1}\ \ P(n)$ is true, where each $P(n)$ is a proposition, it suffices to: **(base step)** show that $P(2)$ is true; and **(induction step)** show that $\forall x \in 2\mathbb{Z}_{\geqslant 1}\ \ (P(x) \Rightarrow P(x+2))$ is true.
7.3.15	(Structural induction over WFF(Σ)). To prove that ∀x ∈ WFF(Σ) P(x) is true, where each P(x) is a proposition, it suffices to: **(base step)** show that $P(p)$ is true for every $p \in \Sigma$; **(induction step)** show that $\forall x, y \in \mathrm{WFF}(\Sigma)\ \ (P(x) \wedge P(y) \Rightarrow P({\sim}p) \wedge P((x \wedge y)) \wedge P((x \vee y)))$.
7.3.18	(Structural induction over WFF+(Σ)). To prove that ∀x ∈ WFF+(Σ) P(x) is true, where each P(x) is a proposition, it suffices to: **(base step)** show that $P(p)$ is true for every $p \in \Sigma$; **(induction step)** show that $\forall x, y \in \mathrm{WFF}^+(\Sigma)\ \ (P(x) \wedge P(y) \Rightarrow P((x \wedge y)) \wedge P((x \vee y)))$.
Lemma 7.3.19	Let Σ be a nonempty set. If x ∈ WFF+(Σ), then assigning false to all the elements of Σ makes x evaluate to false.
7.3.20	The set {∧, ∨} is not a complete set of propositional connectives. In other words, for every nonempty set Σ, ∃x ∈ WFF(Σ) ∀y ∈ WFF+(Σ) y ≡/≡ x.
Tut 5 Q1	$1^2 + 2^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1)$.
Tut 5 Q2	Let $x \in \mathbb{R}_{\geqslant -1}$. Prove by induction that $1 + nx \leqslant (1+x)^n$ for all $n \in \mathbb{Z}_{\geqslant 1}$.
Tut 5 Q3	Prove by induction that 3 divides $n^3 + 11n$ for all $n \in \mathbb{Z}_{\geqslant 1}$.

Tut 5 Q4	Let a be an odd integer. Prove by induction that 2^{n+2} divides $a^{2^n}-1$ for all $n \in \mathbb{Z}_{\geqslant 1}$. (Note that $a^{b^c} = a^{(b^c)}$ by convention.)
Tut 5 Q5	$\forall n \in \mathbb{Z}_{\geqslant 8}\ \exists x, y \in \mathbb{Z}_{\geqslant 0}\ (n = 3x + 5y)$. (As a consequence, any integer-valued transaction over 8 dollars can be carried out using only 3-dollar and 5-dollar coins.)
Tut 5 Q6	Prove by induction that every positive integer can be written as a sum of *distinct* non-negative integer powers of 2, i.e., $\forall n \in \mathbb{Z}_{\geqslant 1}\ \exists \ell \in \mathbb{Z}_{\geqslant 1}\ \exists i_1, i_2, \ldots, i_\ell \in \mathbb{Z}_{\geqslant 0}\ (i_1 < i_2 < \cdots < i_\ell \wedge n = 2^{i_1} + 2^{i_2} + \cdots + 2^{i_\ell})$.
Tut 5 Q7	Show that $F_{n+4} = 3F_{n+2} - F_n$ for all $n \in \mathbb{Z}_{\geqslant 0}$.
Tut 5 Q8	Show by induction that $F_{n+1}^2 - F_{n+1}F_n - F_n^2 = (-1)^n$ for every $n \in \mathbb{Z}_{\geqslant 0}$.
Number Theory	
Divisibility	
Lemma 8.1.5.	Let n, d ∈ Z with d ≠ 0. Then d | n if and only if n/d ∈ Z.
Example 8.1.6.	Let n ∈ Z with d ≠ 0. Then 1 | n and n | n because 1 x n = n = n x 1.
Lemma 8.1.9	Let d, n ∈ Z. If d | n, then −d | n and d | −n and −d | −n.
Proposition 8.1.10	Let d, n ∈ Z. If d | n and n ≠ 0, then |d| ≤ |n|.
Proposition 8.1.12	(transitivity of divisibility). Let a, b, c ∈ Z. If a | b and b | c, then a | c.
Lemma 8.1.14	(Closure Lemma (non-standard name)). Let a, b, d, m, n ∈ Z. If d | m and d | n, then d | am + bn.
8.1.16	(Division Theorem). For all n ∈ Z and d ∈ Z +, there exist unique q, r ∈ Z such that n = dq + r and 0 ≤ r < d.
Corollary 8.1.22	Let n ∈ Z. Then n is either even or odd, but not both.
Tut 6 Q1	Let a, b ∈ ℤ. Show that if a | b and b | a, then a = b or a = − b.
Tut 6 Q5	Let n ∈ ℤ and m = n + 1. m and n have no common prime divisor.
Tut 6 Q6	An integer n is said to be a perfect square if n = k^2 for some k ∈ ℤ. Prove that a positive integer n is a perfect square if and only if it has an odd number of positive divisors. (Hint: pair up the divisors strictly bigger than √n and the divisors strictly smaller than √n.)
Tut 6 Q9	Let $n \in \mathbb{Z}_{\geqslant 1}$ with decimal representation $(a_\ell a_{\ell-1} \ldots a_0)_{10}$. Prove that $9 \mid n$ if and only if $9 \mid (a_0 + a_1 + \cdots + a_\ell)$. This means that a number 9 | n ⇔ 9 | (the sum of digits of n). $10^i = 9 \times 10^{i-1} + 9 \times 10^{i-2} + \cdots + 9 \times 10^0 + 1$ for all $i \in \mathbb{Z}_{\geqslant 0}$.)
Prime Numbers	
Lemma 8.2.4	An integer n is composite if and only if n has a divisor d such that 1 < d < n.
Lemma 8.2.5	(Prime Divisor Lemma (non-standard name)). Let n ∈ Z≥2. Then n has a prime divisor.
Proposition 8.2.6	Let n be a composite positive integer. Then n has a prime divisor p ≤ √n.
8.2.8	(Euclid). There are infinitely many prime numbers.
Base-b Representation	
8.3.13	**Theorem 8.3.13.** For any $n \in \mathbb{Z}^+$, there exist unique $\ell \in \mathbb{Z}_{\geqslant 0}$ and $a_0, a_1, \ldots, a_\ell \in \{0, 1, \ldots, b-1\}$ such that $n = a_\ell b^\ell + a_{\ell-1} b^{\ell-1} + \cdots + a_0 b^0$ and $a_\ell \neq 0$.
Greatest Common Divisors	
Exercise 8.4.3.	Let m, n ∈ Z+. Show that m mod n = 0 if and only if gcd(m, n) = n.

Remark 8.4.4.	In view of Proposition 8.1.10, for all m, n ∈ Z, if m ≠ 0 or n ≠ 0, then gcd(m, n) exists and is positive.
Question 8.4.5.	gcd(0, 0) does not exist
Exercise 8.4.6.	Let m, p ∈ Z +. Show that if p is prime, then either gcd(m, p) = 1 or p | m
Exercise 8.4.7.	Let m, n ∈ Z. Show that the common divisors of m and n are exactly the common divisors of |m| and |n|, and hence gcd(m, n) = gcd(|m|, |n|).
Lemma 8.4.11.	If x, y, r ∈ Z such that x mod y = r, then gcd(x, y) = gcd(y, r).
Tut 7 Q2	Let $a, b, c \in \mathbb{Z}$. Suppose $a \mid c$ and $b \mid c$, and $\gcd(a, b) = 1$. Prove that $ab \mid c$.
Tut 7 Q3	Let $a, b, s, t \in \mathbb{Z}$ such that $as + bt = 1$. Show that $\gcd(a, b) = 1$.
Tut 7 Q4	Let $a, b, s, t \in \mathbb{Z}$ s.t. $as + bt = \gcd(a, b)$. Show that $\gcd(s, t) = 1$.
Tut 7 Q5	Let $a, b \in \mathbb{Z}$ with $a \neq 0$ *or* $b \neq 0$. Prove that $$\gcd\left(\frac{a}{\gcd(a, b)}, \frac{b}{\gcd(a, b)}\right) = 1$$
Tut 7 Q6	Let $a, b \in \mathbb{Z}$ with $a \neq 0$ *or* $b \neq 0$. Prove that an integer n is an integer linear combination of a and b if and only if $\gcd(a, b) \mid n$.
	Fundamental Theorem of Arithmetic
8.5.2.	(Bezout's Lemma). Let m, n ∈ Z with n ≠ 0. Then gcd(m, n) is an integer linear combination of m and n.
Remark 8.5.4.	Let m, n ∈ Z +. If s, t ∈ Z such that gcd(m, n) = ms + nt, then by Exercise 8.4.7, • gcd(−m, n) = gcd(m, n) = ms + nt = (−m)(−s) + nt; • gcd(m, −n) = gcd(m, n) = ms + nt = ms + (−n)(−t); and • gcd(−m, −n) = gcd(m, n) = ms + nt = (−m)(−s) + (−n)(−t).
8.5.5.	(Euclid's Lemma). Let m, n, p ∈ Z +. If p is prime and p | mn, then p | m or p | n.
Assignment 2 Q2	Let $a \in \mathbb{Z}_{\geqslant 2}$. Suppose that for all $m, n \in \mathbb{Z}^+$, if $a \mid mn$, then $a \mid m$ or $a \mid n$. Show that a is prime.
Corollary 8.5.6.	Corollary 8.5.6. Let $n, m_0, m_1, \ldots, m_n, p \in \mathbb{Z}^+$. If p is prime and $p \mid m_0 m_1 \ldots m_n$, then $p \mid m_i$ for some $i \in \{0, 1, \ldots, n\}$.
8.5.9	(Fundamental Theorem of Arithmetic, aka Prime Factorization Theorem). Every integer n ≥ 2 has a unique prime factorization in which the prime factors are arranged in nondecreasing order. • Unique due to "nondecreasing" and the exclusion of 1
	Modular Arithmetic
Lemma 8.6.2.	(alternative definitions of congruence). The following are equivalent for all a, b ∈ Z and all n ∈ Z + (i) a ≡ b (mod n). (ii) a = nk + b for some k ∈ Z. (iii) n | (a − b).
Lemma 8.6.5.	Let a, b, c ∈ Z and n ∈ Z +. (1) (Reflexivity) a ≡ a (mod n). (2) (Symmetry) If a ≡ b (mod n), then b ≡ a (mod n). (3) (Transitivity) If a ≡ b (mod n) and b ≡ c (mod n), then a ≡ c (mod n).
Proposition 8.6.6.	Let a, b, c, d ∈ Z and n ∈ Z + such that a ≡ b (mod n) and c ≡ d (mod n). Then a + c ≡ b + d (mod n).
Proposition 8.6.10.	Let a, b ∈ Z and n ∈ Z +. (1) −a is an additive inverse of a modulo n. (2) b is an additive inverse of a modulo n if and only if b ≡ −a (mod n).
Corollary 8.6.11.	Let n ∈ Z +. If a, b, c ∈ Z such that b + a ≡ c + a (mod n), then b ≡ c (mod n).
Corollary 8.6.12.	Let a, b, x ∈ Z and n ∈ Z +. Then x + a ≡ b (mod n) if and only if x ≡ b − a (mod n).

Proposition 8.6.13.	Let a, b, c, d ∈ Z and n ∈ Z + such that a ≡ b (mod n) and c ≡ d (mod n). Then ac ≡ bd (mod n).
Proposition 8.6.16.	Let a ∈ Z and n ∈ Z +. (1) Let b, b' be multiplicative inverses of a modulo n. Then b ≡ b' (mod n). (2) Let b be a multiplicative inverse of a modulo n and b' ∈ Z such that b ≡ b' (mod n). Then b' is also a multiplicative inverse of a modulo n.
8.6.19.	Let a ∈ Z and n ∈ Z +. Then a has a multiplicative inverse modulo n if and only if a and n are coprime
Corollary 8.6.22.	Let n ∈ Z +. If a, c, d ∈ Z such that ca ≡ da (mod n) and gcd(a, n) = 1, then c ≡ d (mod n).
Corollary 8.6.23	Let n ∈ Z +. Suppose a, b, c ∈ Z, where b is a multiplicative inverse of a modulo n. Then ax ≡ c (mod n) ⇔ x ≡ bc (mod n).
	Relations
Proposition 9.2.13.	Let R be an equivalence relation on a set A. The following are equivalent for all x, y ∈ A. (i) x R y. (ii) [x] = [y]. (iii) [x] ∩ [y] 6= ∅.
9.3.4.	Let R be an equivalence relation on a set A. Then A/R is a partition of A.
9.3.5.	Let C be a partition of a set A. Then there is an equivalence relation R on A such that A/R = C.
Example 9.5.3.	(1) Q+ under the non-strict less-than relation ≤ has neither a minimal element nor a maximal element. (2) Z + under the non-strict less-than relation ≤ has a smallest element but no maximal element.
Lemma 9.5.5.	Consider a partial order ⪯ on a set A. (1) A smallest element is minimal. (2) There is at most one smallest element.
Exercise 9.5.6.	Consider a partial order ⪯ on a set A. (1) A largest element is maximal. (2) There is at most one largest element.
Proposition 9.5.7.	With respect to any partial order ⪯ on a nonempty finite set A, one can find a minimal element.
Exercise 9.5.8.	With respect to any partial order ⪯ on a nonempty finite set A, one can find a maximal element.
9.5.9.	Let A be a set and ⪯ be a partial order on A. Then there exists a total order ⪯* on A such that for all x, y ∈ A, x ⪯ y ⇒ x ⪯* y.
Tut 8 Q2	Let R be a relation on set A. Show that R is symmetric $\Leftrightarrow R = R^{-1}$.
Note to self	A relation can be both symmetric and antisymmetric and it can be neither (but in most cases, it is either one). Have a vertex for every element of the set. Draw an edge with an arrow from a vertex a to a vertex b iff a is related to b (i.e. aRb, or equivalently (a,b) ∈ R). If an element is related to itself, draw a *loop*, and if a is related to b and b is related to a, instead of drawing a parallel edge, reuse the previous edge and just make the arrow double sided (↔) For example, for the set {1,2,3}{1,2,3} the relation R = {(1,1),(1,2),(2,3),(3,2)} has the following graph:



	set theoretical	graph theoretical
Symmetric	If aRb then bRa	All arrows (not loops) are double sided
Anti-Symmetric	If aRb and bRa then $a = b$	All arrows (not loops) are single sided

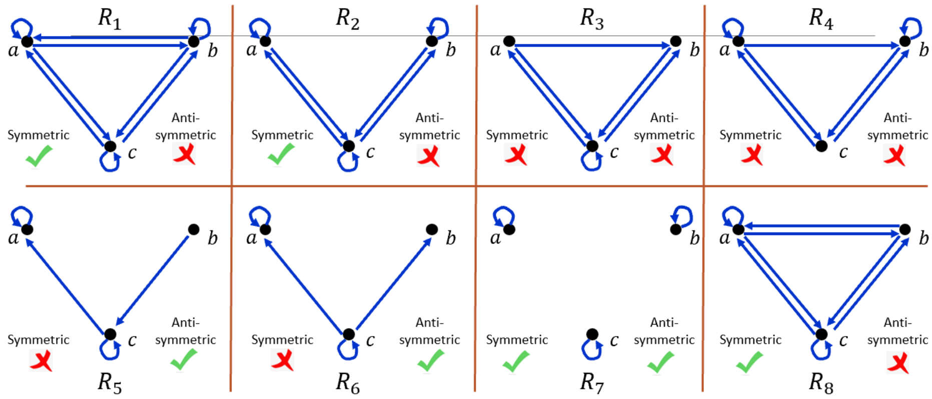
You see then that if there are *any* edges (not loops) they cannot simultaneously be double-sided and single-sided, but loops don't matter for either definition. Any relation on a set A that is both anti-symmetric and symmetric then has its graph consisting of only loops (i.e. is of the form $R = \{(a, a) \mid a \in S \subseteq A\}$ for some $S \subseteq A$.

Any relation whose graph contains *both* types of arrows (single-sided *and* doublesided) will be neither symmetric nor antisymmetric.

Partial orders

R is symmetric: $\forall x, y \in A\ (xRy \Rightarrow yRx)$.
R is antisymmetric: $\forall x, y \in A\ (xRy \wedge yRx \Rightarrow x = y)$.

Definition 9.4.1
Let A be a set and R be a relation on A.
R is a partial order if R is reflexive, antisymmetric and transitive.



Tut 8 Q5

Let A, B be nonempty sets and $f: A \to B$ be a surjection. Show that $\mathcal{C}$ is a partition on A where

$$\mathcal{C} = \{\{x \in A: f(x) = y\} : y \in B\}$$

Observations:
(1) The components of $\mathcal{C}$ are pairwise disjoint.
(2) Union of all the components of $\mathcal{C}$ is A.

Assignment Q5

Let $\mathcal{C}$ be a partition of a set A. Show that there exist a set B and a surjection $f: A \to B$ such that

$$\mathcal{C} = \{\{x \in A: f(x) = y\} : y \in B\}$$

Tut 8 Q7

Let $\preccurlyeq$ be a partial order on a set P, and a, $b \in P$

- a, b are **comparable** if $a \preccurlyeq b$ or $b \preccurlyeq a$.
- a, b are **compatible** if $\exists c \in P$ such that $a \preccurlyeq c$ and $b \preccurlyeq c$.

- in all partially ordered sets, any two comparable elements are compatible.
- But it is not true that any two compatible elements are comparable.

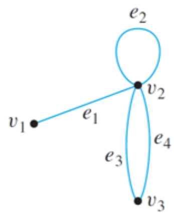
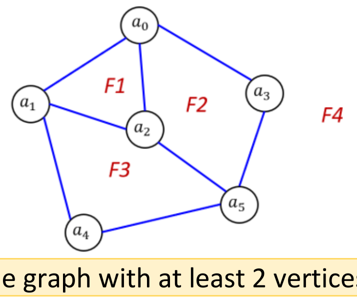
Counting and Probability

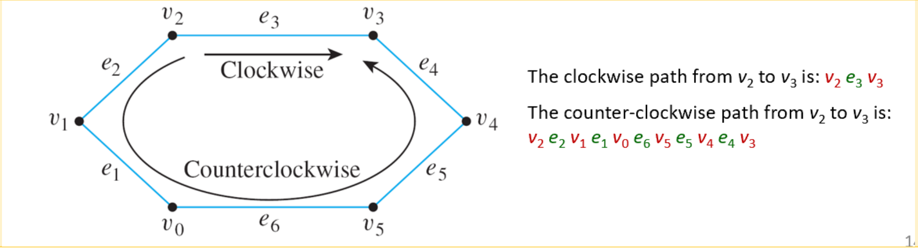
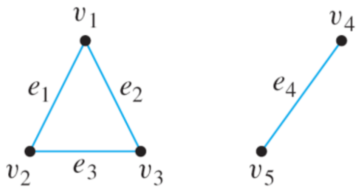
9.1.1. (The Number of Elements in a List)
If m and n are integers and $m \leq n$, then there are $n - m + 1$ integers from m to n inclusive.

9.2.1. (The Multiplication/Product Rule)

	If an operation consists of k steps and • the first step can be performed in n_1 ways, • the second step can be performed in n_2 ways (regardless of how the first step was performed), • the k^{th} step can be performed in n_k ways (regardless of how the preceding steps were performed), Then the entire operation can be performed in $\boldsymbol{n_1 \times n_2 \times n_3 \times \ldots \times n_k}$ ways.
9.2.2.	(Permutations) The number of permutations of a set with n ($n \geq 1$) elements is $\boldsymbol{n!}$
9.2.3.	(r-permutations from a set of n elements) If n and r are integers and $1 \leq r \leq n$, then the number of r-permutations of a set of n elements is given by the formula $$P(n,r) = n(n-1)(n-2)\ldots(n-r+1) = \frac{n!}{(n-r)!}$$
9.3.1.	(The Addition/Sum Rule) Suppose a finite set A equals the union of k distinct mutually disjoint subsets $A_1, A_2, \ldots, A_k$. Then $\|A\| = \|A_1\| + \|A_2\| + \ldots + \|A_k\|$.
9.3.2.	(The Difference Rule) If A is a finite set and $B \subseteq A$, then $\|A \setminus B\| = \|A\| - \|B\|$.
9.3.3.	If A, B, and C are any finite sets, then $\|A \cup B\| = \|A\| + \|B\| - \|A \cap B\|$ and $\|A \cup B \cup C\| = \|A\| + \|B\| + \|C\| - \|A \cap B\| - \|A \cap C\| - \|B \cap C\| + \|A \cap B \cap C\|$
Pigeonhole Principle (PHP)	A function from one finite set to a smaller finite set cannot be one-to-one: There must be at least 2 elements in the domain that have the same image in the co-domain.
Generalized PHP	• For any function f from a finite set X with n elements to a finite set Y with m elements and for any positive integer k, if $k < n/m$, then there is some $y \in Y$ such that y is the image of at least $k + 1$ distinct elements of X. • (Contrapositive) For any function f from a finite set X with n elements to a finite set Y with m elements and for any positive integer k, if for each $y \in Y$, $f^{-1}(\{y\})$ has at most k elements, then X has at most km elements; in other words, $n \leq km$.
9.5.1.	The number of subsets of size r (or r-combinations) that can be chosen from a set of n elements, $\binom{n}{r}$, is given by the formula $$\binom{n}{r} = \frac{P(n,\ r)}{r!} = \frac{n!}{r!\,(n-r)!}$$ where n and r are non-negative integers with $r \leq n$.
9.5.2.	(Permutations with sets of indistinguishable objects) Suppose a collection consists of n objects of which • n_1 are of type 1 and are indistinguishable from each other • n_2 are of type 2 and are indistinguishable from each other… • n_k are of type k and are indistinguishable from each other • and suppose that $n_1 + n_2 + \ldots + n_k = n$. Then the number of distinguishable permutations of the n objects is $$\binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\cdots\binom{n-n_1-n_2-\cdots-n_{k-1}}{n_k} = \frac{n!}{n_1!\,n_2!\,n_3!\cdots n_k!}$$
9.6.1.	(Number of r-combinations with Repetition Allowed) The number of r-combination with repetition allowed (multisets of size r) that can be selected from a set of n elements is:

	$$\binom{r+n-1}{r}$$ This equals the number of ways r objects can be selected from n categories of objects with repetitions allowed.
9.7.1.	(Pascal's Formula) Let n and r be positive integers, $r \leq n$. Then $$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$$
9.7.2.	(Binomial Theorem) Given any real numbers a and b and any non-negative integer n, $$\begin{aligned}(a+b)^n &= \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \\ &= a^n + \binom{n}{1} a^{n-1} b^1 + \binom{n}{2} a^{n-2} b^2 + \cdots + \binom{n}{n-1} a^1 b^{n-1} + b^n\end{aligned}$$
6.3.1 (Epp) 5.2.4. (Lawrence)	(No. of elements in a Power Set) If a set X has n ($n \geq 0$) elements, then $\wp(X)$ has 2^n elements.
9.9.1.	(Bayes' Theorem) Suppose that a sample space S is a union of mutually disjoint events $B_1, B_2, B_3, \ldots, B_n$. Suppose A is an event in S, and suppose A and all the B_i have non-zero probabilities. If k is an integer with $1 \leq k \leq n$, then $$P(B_k\|A) = \frac{P(A\|B_k) \cdot P(B_k)}{P(A\|B_1) \cdot P(B_1) + P(A\|B_2) \cdot P(B_2) + \cdots + P(A\|B_n) \cdot P(B_n)}$$
Tut 9 Q6	How many possible functions $f: A \to B$ are there if $\|A\| = n$ and $\|B\| = k$? • Each of the n elements in A must be mapped to one of the k elements in B. • Therefore, there are k^n possible functions f.
Tut 10 Q3	$\binom{m+n}{r} = \binom{m}{0}\binom{n}{r} + \binom{m}{1}\binom{n}{r-1} + \cdots + \binom{m}{r}\binom{n}{0}$ where $m, n \in \mathbb{Z}^+, r \leq m$ and $r \leq n$. Then, for all integers $n \geq 0$, $$\binom{2n}{n} = \binom{n}{0}^2 + \binom{n}{1}^2 + \cdots + \binom{n}{n}^2$$
	Graphs
10.1.1.	(The Handshake Theorem) If the vertices of G are $v_1, v_2, \ldots, v_n$, where $n \geq 0$, then the total degree of G = deg(v_1) + deg(v_2) + … + deg(v_n) = 2 × (the number of edges of G).
Corollary 10.1.2.	The total degree of a graph is even.
Proposition 10.1.3.	In any graph, there are an even number of vertices of odd degree.
Lemma 10.2.1.	Let G be a graph. a. If G is connected, then any two distinct vertices of G can be connected by a path. b. If vertices v and w are part of a circuit in G and one edge is removed from the circuit, then there still exists a trail from v to w in G. c. If G is connected and G contains a circuit, then an edge of the circuit can be removed without disconnecting G.
10.2.2.	If a graph has an Euler circuit, then every vertex of the graph has positive even degree. • (Contrapositive) If some vertex of a graph has odd degree, then the graph doesn't have an Euler circuit.
10.2.3.	If a graph G is <u>connected</u> and the degree of every vertex of G is a positive <u>even integer</u>, then G has an Euler circuit.
10.2.4.	(combining 10.2.2. and 10.2.3.)

	A graph *G* has an Euler circuit iff *G* is connected and every vertex of *G* has positive even degree.
Corollary 10.2.5	Let *G* be a graph, and let *v* and *w* be two distinct vertices of *G*. There is an Euler trail from *v* to *w* if and only if *G* is connected, *v* and *w* have odd degree, and all other vertices of *G* have positive even degree.
Proposition 10.2.6.	If a graph *G* has a Hamiltonian circuit, then *G* has a subgraph *H* with the following properties: 1. *H* contains every vertex of *G*. 2. *H* is connected. 3. *H* has the same number of edges as vertices. 4. Every vertex of *H* has degree 2.
10.3.2.	If *G* is a graph with vertices $v_1, v_2, \ldots, v_m$ and **A** is the adjacency matrix of *G*, then for each positive integer *n* and for all integers $i, j = 1, 2, \ldots, m$, the *ij*-th entry of $\mathbf{A}^n$ = the number of walks of length *n* from v_i to v_j. **Consider the adjacency matrix A of the graph *G*.** $\mathbf{A} = \begin{array}{c c} & \begin{array}{ccc} v_1 & v_2 & v_3 \end{array} \\ \begin{array}{c} v_1 \\ v_2 \\ v_3 \end{array} & \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 2 \\ 0 & 2 & 0 \end{bmatrix} \end{array}.$  Compute $\mathbf{A}^2$: $\begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 2 \\ 0 & 2 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 2 \\ 0 & 2 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 2 \\ 1 & 6 & 2 \\ 2 & 2 & 4 \end{bmatrix}.$ Note that the entry in row 2 and column 2 is 6, which equals the number of walks of length 2 from v_2 to v_2. To compute a_{22}, you multiply row 2 of A with column 2 of A to obtain a sum of three terms: $\begin{bmatrix} 1 & 1 & 2 \end{bmatrix}\begin{bmatrix} 1 \\ 1 \\ 2 \end{bmatrix} = 1\cdot 1 + 1\cdot 1 + 2\cdot 2.$
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*.
Kuratowski's Theorem	A finite graph is planar if and only if it does not contain a subgraph that is a subdivision of the complete graph K_5 or the complete bipartite graph $K_{3,3}$.
Euler's Formula	For a connected planar simple graph $G = (V, E)$ with $e = \lvert E\rvert$ and $v = \lvert V\rvert$, if we let *f* be the number of faces, then $f = e - v + 2$.  $e = 8$ $v = 6$ $f = 8 - 6 + 2 = 4$
Tut 11 Q2	Show that every simple graph with at least 2 vertices has two vertices of the same degree.
Tut 11 Q4	Prove that for any simple graph G with 6 vertices, G or its complementary graph $\bar{G}$ contains a triangle.
	Trees
Lemma 10.5.1	Any non-trivial tree has at least one vertex of degree 1.
10.5.2.	Any tree with *n* vertices ($n > 0$) has $n - 1$ edges.
Exercise	Using Theorem 10.5.2, prove that a non-trivial tree has at least 2 vertices of degree 1.
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.

	
10.5.4.	If G is a connected graph with n vertices and $n – 1$ edges, then G is a tree. • Note that although it is true that every *connected* graph with n vertices and $n – 1$ edges is a tree, it is not true that *every* graph with n vertices and $n – 1$ edges is a tree. • E.g. this following graph has 5 vertices and 4 edges but it is not a tree 
10.6.1.	(Full Binary Tree Theorem) If T is a full binary tree with k internal vertices, then T has a total of $2k + 1$ vertices and has $k + 1$ terminal vertices (leaves).
10.6.2.	For non-negative integers h, if T is any binary tree with height h and t terminal vertices (leaves), then $t \leq 2^h$ Equivalently, $\log_2 t \leq h$
Proposition 10.7.1	1. Every connected graph has a spanning tree. 2. Any two spanning trees for a graph have the same number of edges.

Definition	**Symbol / Meaning**
Even integer	n is even $\Leftrightarrow \exists$ an integer k such that $n = 2k$ (iff)
Odd integer	n is odd $\Leftrightarrow \exists$ an integer k such that $n = 2k + 1$ (iff)
Prime integer	An integer n is prime iff $n > 1$ and for all positive integers r and s, if $n = rs$, then either r or s equals n. $\forall r, s \in \mathbb{Z}^+$, if $n = rs$ then either $r = 1$ and $s = n$ or $r = n$ and $s = 1$.
Composite integer	An integer n is composite iff $n > 1$ and $n = rs$ for some integers r and s with $1 < r < n$ and $1 < s < n$. $\exists\, r, s \in \mathbb{Z}^+$ s.t. $n = rs$ and $1 < r < n$ and $1 < s < n$.
Rational No.	A real number r is rational if, and only if, it can be expressed as a quotient of two integers with a nonzero denominator. A real number that is not rational is irrational. r is rational $\Leftrightarrow \exists$ integers a and b such that $r = \frac{a}{b}$ and $b \neq 0$.
Divisibility	If n and d are integers and $d \neq 0$, then n is divisible by d iff n equals d times some integer. $d \mid n$: "d divides n". Symbolically, if $n,\ d \in \mathbb{Z}$ and $d \neq 0$: $d \mid n \Leftrightarrow \exists k \in \mathbb{Z}$ such that $n = dk$.

Common mistakes	Wrong e.g.	Explanation
All birds can fly. **∀*x*, (Bird(*x*) → Fly(*x*))**	∀*x*, Fly(Bird(*x*))	Bird(*x*) is a **predicate**; it evaluates to true or false. This is like writing Fly(true) or Fly(false), which makes no sense.
	∀*x*, (Bird(*x*) ∧ Fly(*x*))	This is saying everything must be a bird and it flies.
There is a bird that can fly. **∃*x* s.t. (Bird(*x*) ∧ Fly(*x*))**	∃*x* s.t. (Bird(*x*) → Fly(*x*))	If there are no birds at all → vacuously true (not the case)
Not all birds can fly. **(negation of the 1st one)** **∃*x* s.t. (Bird(*x*) ∧ ~Fly(*x*))**	∀*x*, (Bird(*x*) → ~Fly(*x*))	All birds cannot fly
	∃*x* s.t. (Bird(*x*) → ~Fly(*x*))	Becomes a vacuously true case if there are no birds