MATH1081 notes

Nira (z5417727)

September 17th, 2022

Contents

1 Topic 1

1.1 Introduction

1. addition, multiplication, division and subtraction
2. Mainly dealing with finite sets

1.2 Sets and subsets

A set is a well defined collection of distinct objects

Example: $S = \{1, a, 3\}, A = \{\Pi, 1\}$.
1. $e \notin A$; it is not in A
2. For example, if A is a set of all integers; {all even integers} $= \{n \in \mathbb{R} | \text{n is even}\}$.
3. We can remove superfluos items (elements that occur more than one). $A = \{1, 2, 3, 3\}$ where 3 can be removed.

Example:
$A = \{1, 2, 3\}, B = \{2, 3, 1\}, C = \{1, 2, 3, 3\}, D = \{1, 3\}$.
Here, D is a proper subset of A, B, C; A, B, C are supersets of D.
$\subseteq$: Subset (proper subset),$\supseteq$: Superset.

1. To prove if a set is a proper subset; do the following:
For example, if $D \in A$, then check if $e \in D$
If $e \in D$, then $e \in A$. Thus, it would be a proper subset (here, e is just an element).

2. To prove that two sets are equal;
For example, if A = B, prove:
i) $A \subseteq B$; if an element is in A, then the element is in B.
ii) $B \subseteq A$; if an element is in B, then the element is in A.

1.3 Power Sets and Stability

Subsets of $A = \{1, 2, 3\}$:
1. Could throw everything out to get empty set Φ,
2. One element each: $\{1\}, \{2\}, \{3\}$,
3. Two elements: $\{1, 2\}, \{2, 3\}, \{1, 3\}$,
4. Set itself: A.
The set containing 1, 2, 3, 4 is called the powerset of A.

Given $A = \{1, 2, 3\}, B = \{1, 2, 3, 3\}, C = \{1, 3\}, D = \{1, 3\}$, where $A = B$, $C \subseteq A, B$ and $D \nsubseteq A, B, C$.
1. size of A = 3, B = 3, C = 2, D = 2.
[Exercise with A = 0, 1, 0, 1, B done in word].

1.4 Set Operations

Boolean Operators ("not" operation in programming):
1. Complement:
Let there be a set A in U (A: all of the people in the video, U: universal set of everyone in the world, A^c = complement of A).

$$\boxed{A^c = \{x \in U | x \notin A\}.}$$

2. Intersecting ("and" operation in programming):
If there is A, B, intersecting,

$$\boxed{A \cap B = \{x \in A | x \in B\}.}$$

3. Union ("or" operation in programming): If there is A, B, A or B is:

$$\boxed{A \cup B = \{x \in U | x \in A \text{ or } x \in B\}.}$$

4. Difference: If there is A, B, intersecting,

$$\boxed{A - B = \{x \in A | x \in B\}.}$$

[examples in word doc]

1.5 The Inclusion-Exclusion Principle

[example in Word]

$$\boxed{|A \cup B| = |A| + |B| - |A \cap B|.}$$

For three elements,

$$\boxed{|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.}$$

[example in word]

1.6 Sets Proofs

[proof question in word]
Hints for proofs:
1. To prove that $S \subseteq T$, we can assume that $x \in S$ and show that $x \in T$.
2. To prove that $S = T$, we can show that $S \subseteq T$ and $T \subseteq S$.

Scaffold:

Proof: Suppose that ..... (proof)we see that/ it follows ... (conclusion) (end with shaded box to indicat

Note that the "Suppose that" part of the proof is usually whatever the if statment mentions.

For example, if the question is "Prove that if $A \cap B = A$, then $A \cup B = B$, then the proof starts like this:

$\underline{Proof}$: Suppose that $A \cap B = A$.

For questions like "is this statement true", there are two ways to approach the question:
1. If the statement is true (if you think it is true), then prove it.
2. If the statement is false, then give a counter-example that proves it false.
[examples in word]

1.7 Laws of Set Algebra

Laws of Set Algebra

1. $A \cap B = B \cap A$: Commutative Law.
2. $A \cap (B \cap C) = (A \cap B) \cap C$: Associative Law.
3. $A \cap (B \cap C) = (A \cap B) \cup (A \cap C)$: Distributive Law.
4. $A \cap (A \cap B) = A$: Absorption Law.
5. $A \cap U = U \cap A = A$: Identity Law.
6. $A \cap A = A$: Idempotent Law.
7. $(A^c)^c = A$: Double Complement Law.
8. $A \cap \emptyset = \emptyset \cap A = \emptyset$: Domination Law.
9. $A \cap A^c = \emptyset$: Intersection with Complement Law.
10. $(A \cup B)^c = A^c \cap B^c$: De Moirve's Law.

The intersection can be swapped with the union to form another law (like, $A \cup B = B \cup A$ swapped as $A \cap B = B \cap A$.). Similarily, U should be swapped with $\emptyset$ and vice versa.
[examples in word]

1.8 Generalised Set Operations

Unions and Intersections; A saga:

1. $\cup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cap A_n$,
2. $\cap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \cdots \cap A_n$.

Example:

$$A_k = k, k+1;$$
$$= \cup_{i=1}^{3} A_k = A_1(\{1,2\}) \cup A_2(\{2,3\}) \cup A_3(\{3,4\}),$$
$$= \{1,2,3,4\}.$$

[example in word]

1.9 Russel's Paradox

A set may contain another set as one of its elements.
This raises the possibility that a set may contain itself as an element.

Problem: Try to let S be the set of all sets that are not elements of themselves, i.e., $\mathbf{S} = \{\mathbf{A} | \mathbf{A}$ is a set and $\mathbf{A} \notin \mathbf{A}\}$.
Is S an element of itself?
i) If $S \in S$, then the definition of S implies that $S \notin S$, a contradiction.
ii) If $S \notin S$, then the definition of S implies that $S \in S$, also a contradiction.
Hence neither $S \in S$ nor $S \notin S$. This is Russell's paradox.

1.10 Cartesian Product

[example in word]
The Cartesian product of two sets A and B, denoted by $A \times B$, is the set of all ordered pairs from A to B:

$$\boxed{A \times B = \{(a, b) | a \in A \text{ and } b \in B\}}$$

If $|A| = m$ and $|B| = n$, then we have $|A \times B| = mn$.

Sets with more than 2 elements:

Example: $A = \{a, b\}, B = \{1, 2, 3\}$.

$$\text{Cartesian Product } (A \times B) = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$$

(all of the ordered pairs – combinations)

[example in word]

When X and Y are small finite sets, we can use an arrow diagram to represent a subset S of $X \times Y$: we list the elements of X and the elements of Y , and then we draw an arrow from x to y for each pair $(x, y) \in S$.

1.11 Functions

Example: Take 2 sets X and Y, for which we have to find a function.

$$X = \{\text{all MATH 1081 students}\}, Y = \{0, 1, \ldots, 84, 85, \ldots, 100\}.$$

X: number of students; Y: marks from $0 - 100$.
Take function $f : X \to Y$; where X is the domain and Y is the co domain.
Ie, $f(x) =$ X's mark (Y).
Function $f : X \to Y$ satisfies $\{(x, f(x))|x \in X\} \subseteq X \times Y$ so that, for each $x \in X$;
1. $f(x)$ exists
2. $f(x)$ is unique

[example in word]

Note: be vary of the one-to-one function property lol

Floor function and ceiling functions:

1. Floor function (rounds down; smallest integer):

$$\lfloor x \rfloor = \max \{z \in Z | z \leq x\}.$$

2. Ceiling function (rounds up; largest integer):

$$\lceil x \rceil = \min \{z \in Z | z \geq x\}.$$

[example in word] Domain/codomain: $\lfloor x \rfloor / \lceil x \rceil : \mathbb{R} \to \mathbb{Z}$.

Range($\lceil x \rceil$) $= \mathbb{Z}$.

[example in word]

1.12 Image and Inverse Image

- The image of a set $A \subseteq X$ under a function $f : X \to Y$ is $f(A) = \{y \in Y \text{ — } y = f(x) \text{ for some } x \in A\} = \{f(x)|x \in A\}$.

- The inverse image of a set $B \subseteq Y$ under a function $f : X \to Y is f^{-1}(B) = \{x \in X|f(x) \in B\}$.

(image is just function values in the doman and inverse image is function values in range).

note: this is just function and inverse functions.

[example in word]

1.13 Injective, Surjective, Bijective

Formal Definitions:

Recall that if f is a function from X to Y , then for every $x \in X$, there is exactly one $y \in Y$ such that $f(x) = y$.

1. We say that a function $f : X \to Y$ is injective or one-to-one if, for every $y \in Y$, there is at most one $x \in X$ such that $f(x) = y$.
Example: for all $x_1, x_2 \in X$, if $f(x_1) = f(x_2)$ then $x_1 = x_2$.

2. We say that a function $f : X \to Y$ is surjective or onto if, for every $y \in Y$, there is at least one $x \in X$ such that $f(x) = y$. the range of f is the same as the codomain of f (range(f) = Y).

3. We say that a function $f : X \to Y$ is bijective if f is both injective and surjective (one-to-one and onto).

for every $y \in Y$, there is exactly one $x \in X$ such that $f(x) = y$.
[example in word]

1.14 Composition of Functions

For functions $f : X \to Y$ and $g : Y \to Z$, the composite of f and g is the function $g \circ f : X \to Z$ defined by $(g \circ f)(x) = g(f(x))$ for all $x \in X$.

The composite function $g \circ f$ exists whenever the range of f is a subset of the domain of g.

In general, $g \circ f$ and $f \circ g$ are not the same composite functions. Associativity of composition (assuming they exist): $h \circ (g \circ f) = (h \circ g) \circ f$.

Example: Take sets $X = \{$ **all MATH1081 students** $\}, Y = \{0, 1, \ldots, 100\}, Z = \{F, P, CR, D, HD\}$.

Maps: $f = X \to Y; g = Y \to Z$.

A) $g \circ f : X \to Z$.
$(f \circ g)(y) = f(g(y))$.
[examples in word]

1.15 Identity and Inverse Functions

Identity Function:

$\boxed{i_x : x \to x; i_x(x) = x.}$

For any function $f : X \to Y$, we have $f \circ i_x = f = i_y \circ f$. A function $g : Y \to X$ is an inverse of $f : X \to Y$ if $g(f(x)) = x$ for all $x \in X$ and $f(g(y)) = y$ for all $y \in Y$,
or equivalently, $g \circ f = i_x$ and $f \circ g = i_y$.

$\boxed{\text{1. A function can have at most one inverse.}}$

If $f : X \to Y$ has an inverse, then we say that f is invertible, and we denote the inverse off by f^{-1}. Thus,$f^{-1} \circ f = i_x$ and $f \circ f^{-1} = i_y$.

If g is the inverse of f, then f is the inverse of g. Thus, $(f^{-1})^{-1} = f$.

[example in word]

1.16 Inverse Function Proofs

Theorem and Proof:

1. A function $f : X \to Y$ has at most 1 inverse

Proof:

$$\begin{aligned} &\text{Let } g_1, g_2 : Y \to X \text{ be inverse of } f. \\ &\text{Then } : g_1 = g_i \circ i_y \\ &= g_i \circ (f \circ g_2) \\ &= (g_i \circ f) \circ g_2 \\ &= i_x \circ g_2 \\ &= g_2 \text{ End of proof .} \end{aligned}$$

[example in word]

2 Number Theory and Relations

2.1 Numbers and Divisibility

[topic 2 done in word (SteelsSlides1): maybe put in definitions here ?? that depends]

Number Set Notation:

1. The positive integers: $\mathbb{Z}^+ = \{1, 2, 3, \dots\}$,
2. The natural numbers: $\mathbb{N} = \{0, 1, 2, 3, \dots\}$,
3. The integers: $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$,
4. The rational numbers: $\mathbb{Q} = \{m/n : m \in \mathbb{Z}, n \in \mathbb{Z}^+\}$,
5. The real numbers, $\mathbb{R}$ and the complex numbers $\mathbb{C}$.

Tests (Divisibility):

1. 2 — N if and only if the decimal expansion of N ends in an even integer
2. 5 — N if and only if the last decimal digit of N is 5 or 0.
3. 3 — N if and only if the sum of the decimal digits of N is divisible by 3.
3': 9 — N if and only if the sum of the decimal digits of N is divisible by 9.
4. 11 — Nif the alternating sum of the decimal digits of N is divisible by 11. (example: $1232 = 1 - 2 + 3 - 2 = 0$)

[proof in word]

2.2 Primes

[in word]

Primes Definition: Formal: Another way of saying this is if p is prime:

$$x \text{ — } p \text{ implies } x \in \{-1, 1, -p, p\}$$

.

Theorems:

1. If p is prime and $p|ab$, then $p|a$ or $p|b$,
2. If n is composite, then it has a prime factor less than or equal to $\sqrt[2]{n}$,
3. If no prime less than or equal to $\sqrt[2]{n}$ divides n then n is a prime,
4. Every integer $n \geq 2$ can be written uniquely as a product of a finite number of primes in increasing order i.e. $n = p_1^{m_1} * p_2^{m_2} \dots p_k^{m_k}$ for primes $p_1 < p_2 < \cdots < p_k$ and exponents $m_1, m_2, \dots, m_k \in \mathbb{Z}^+$.

Open Results about Primes:

1. A prime of the form $2^n + 1$ is called a Fermat prime.
2. A prime of the form $2^n - 1$ is called a Mersenne prime.
3. Two primes that differ by 2, are called twin primes. For example, 3 and 5 are twin primes; so are 29 and 31.
4. The Goldbach Conjecture is that they are: it has been proved true for all numbers with fewer than about 17 digits.

2.3 Common Divisors and Multiples

[mostly on word]
All $a, b \in \mathbb{Z}$ have (at least) one common divisor, namely 1, and so we can define the following:
For $a, b \in \mathbb{Z}$, not both zero, the positive integer d such that

$$1.d \text{ — } aandd \text{ — } b,$$

$$2.If c \text{ — } aandc \text{ — } bthenc \leq d.$$

is called the greatest common divisor of a and b. We write $d = gcd(a, b)$.

Begin by writing a and b as a product of primes.

Properties of GCD:

1. gcd (a, b) is not affected by the signs of a or b
2. Condition (2) in the definition of gcd can be replaced by $(2')$ if c — a and c — b then c — d.
3. For $a \in \mathbb{Z}^+$, gcd $(a, 0) = a$.

Least Common Multiple

All $a, b \in \mathbb{Z}$ have (at least) one common multiple, namely ab, and so we can define the following: For $a, b \in \mathbb{Z}$, not both zero, the positive integer l such that

$$1)a \text{ — } l \text{ and } b \text{ — } l$$

2)If a — c and b — c then $l \leq c$ is called the least common multiple of a and b.

We write $l =$ lcm (a, b).

Theorem:

For all positive integers a and b; gcd$(a, b)x$ lcm $(a, b) = ab$.

Quotient and Remainder

[mostly in word]

The Quotient-Remainder Theorem (aka The Division Algorithm)

If $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$, then there exist unique $q, r \in Z$ such that (q: quotient; r: remainder):

$$a = bq + r \text{ and } 0 \leq r < b.$$

Note: q can be found using floor function; $q = \lfloor a/b \rfloor$.; then $r = a - qb$.

2.4 The Euclidean Algorithm

[mostly in word]

If $a = bq + r$ then $\gcd(a, b) = \gcd(b, r)$.

The Euclidian Algorithm: General Case [steps]

1) Let a and b be integers with $a > b \geq 0$.
2) If $b = 0$, then $\gcd(a, b) = a$.
3) If $b > 0$, use the Quotient-Remainder theorem to write $a = bq + r$ where $0 \leq r < b$. Then by our prevous result, $\gcd(a, b) = \gcd(b, r)$.
4) Repeat steps 2 and 3 to find $\gcd(b, r)$.

Example: Find $\gcd(708, 540)$

$$708 = 540 \cdot 1 + 168,$$

$$540 = 168 \cdot 3 + 36,$$

$$168 = 36 \cdot 4 + 24,$$

$$36 = 24 \cdot 1 + 12,$$

$$24 = 12 \cdot 2 + 0.$$

So,

$$\gcd\ (708, 540) = 12.$$

Note: gcd is the last non-zero remainder.

Bezout's Identity

For $a, b \in Z$ not both zero, there exist integers x and y (not unique) such that:

$\gcd\ (a, b) = ax + by.$

Theorem: Integers a and b are relatively prime if and only if there exists $x, y \in Z$ such that $ax + by = 1$.

Extended Euclidean Theorem: The Extended Euclidean Algorithm is a more efficient way of finding the numbers in Bézout's Identity: In looking for $\gcd(a, b)$, assume $a > b > 0$.
1. We make up a table with five columns labelled i, q_i, r_i, x_i, y_i, where i labels the rows.
2. We set row 1 to be $1, 0, a, 1, 0$ and row 2 to be $2, 0, b, 0, 1$. Thus $q_1 = q_2 = 0; r_1 = a, r_2 = b; x_1 = y_2 = 1; x_2 = y_1 = 0$.
3. Then for i from 3 onwards, q_i is the quotient on dividing r_{i-2} by r_{i-1} (a divided by b in the first case).

4. Then subtract q_i times the rest of row $i-1$ from row $i-2$.
5. Repeat until we get $r_{n+1} = 0$ for some n, then stop. Then the gcd is r_n and $r_n = ax_n + by_n$, that is the last row before r_i was zero gives the gcd, the x and the y.
In fact a similar identity holds at each step: $r_i = ax_i + by_i$.

2.5 Modular Arithmetic

[mostly in word]

Let $m \geq 2$ be an integer. We say that a and b are congruent modulo m if $m|(a-b)$.
We write this as:

$$a \cong b(modm).$$

The reason we have taken our modulus m to be greater than 2 is that
1) As $m|(a-b)$ iff $-m|(a-b)$, there is nothing to be gained from using negative moduli.
2) All numbers are congruent modulo 1, so that is not interesting.
3) divisibility by 0 is not defined.

Theorem
For integers $a, b$and $m, a \cong b(modm)$ if and only if there is an integer k such that $a = b + km$.

Arithmetic with Congrences
Suppose $a \cong b(modm)$ and $c \cong d(modm)$.
Then

$$(1a)(a+c) \cong (b+d)(modm).$$

$$(1b)(a-c) \cong (b-d)(modm).$$

$$(2)ac \cong bd(modm).$$

$$(3)an \cong bn(modm)foralln \in N.$$

$$(4)Ifk — mthena \cong b(modk).$$

$\boxed{note : neverdividecongruences}$

Applications of Congruence Arithmetic:
1. Pseudo-random Numbers
2. Equations with no solutions

2.6 Congruence Equations

(note: just simple forms, yeah?)

Linear Congrence equation form: $ax \equiv b(\mod m)$.

[example in slide07 pdf]

Tricks.
• If, in $ax \equiv b(\mod m)$, $\gcd(a, m) > 1$ but it does not divide a, then the congruence has no solution.
• If $gcd(a, m) = 1$, then it has a unique solution for modulo m.
• Otherwise, divide everything by $d = gcd(a, m)$, then find solutions.
• Once you have a solution; if the equation was divided by d; then the formula for general solutinos is $k + q(m/d) < m$ where k is the first solution and $q \in \mathbb{R} - 0$.

2.7 Relations

Rule of $f : A \to B$ is that takes each element $a \in A$ to exactly one of $b \in B$.

Set A: domain; Set B: codomain

• $f : A \to B$ is also cartesian product of $A \times B$ which contains one and only one ordered pair of (a, b) for each $a \in A$.
• One-to-one function: iff there is at most one pair for every $b \in B$.
• Onto function: iff there is at least one pair for every $b \in B$.

Examples of relations between sets.

• Subset;
• Congruence (between integers or e.g. triangles);
• Divisibility;
• Less than;
• Equality (most important one)!

Relation of AxB; R:

• We call A the domain of R and B the codomain of R.
• If $(a, b) \in R$, we say that a is related to b (by R), written as aRb.
• If $(a, b) \notin R$ we write $a \not R b$.

Relation from set A to itself is called **a relation on A.**

Relation $f : A \to B$ gives: $\{(a, f(a))\} \subseteq A \times B$.

[example in slide 08 pdf]

Ternary Relation on $\mathbb{Z} : \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$. (for AxB, it would be a binary relation).

Can generalise it for 3 sets: $A \times B \times C$; example would be a modular statement like $a \equiv b(\text{ mod } m)$.

Representing relations on finite sets. For finite sets $A = \{a_1, a_2, \ldots a_m\}$ and $B = \{b_1, b_2, \ldots, b_n\}$, describe relation from A to B by:

• Arrow diagrams: dots (vertices) labelled a_i to b_j and join them by an arrow iff $(a_i, b_j) \in \mathbb{R}$.
• Rectangular array of numbers (a matrix) M_R where entry in ith row and jth column is m_{ij} and where: $m_{ij} = 1$ if $(a_i, b_j) \in \mathbb{R}$ and 0 otherwise.

[example in 08 pdf]

•arrow diagrams are sometimes called directed graphs or digraph.

2.8 Properties of Relations

Reflexive Relation:

Reflexive iff $(x, x) \in R$ that is xRx

Drawn as:
• a loop in a vertex in directed graph
• main diagonal is all 1s

[example in slide 9 pdf]

Symmetric Relation:

Symmetric relation R on set A iff $(x, y) \in A$ that is xRy implies yRx

Drawn as:
• arrow pointing both ways (ie $x \leftrightarrow y$) in a directed graph
• matrix M_R is symmetric about main diagonal.

[example in slide 9 pdf]

Antiymmetric Relation:

Antiymmetric relation R on set A iff $(x, y) \in A$ if both xRy and yRx then $x = y$.

Drawn as:
• arrow pointing both ways (ie $x \leftrightarrow y$) in a directed graph should NEVER appear
• matrix M_R if $i \neq j$, then either $m_{ij} = 0$ or $m_{ji} = 0$ (or both).

[example in slide 9 pdf]

Transitive Relation:

Transitive relation R on set A iff for all $x, y, z \in A$, if both xRy and yRx then xRZ.

Drawn as:
• arrow pointing (ie $x \to y \to z; x \to z$) and (if $x \to y$ then x and y must be reflexive) in a directed graph
• matrix M_R, each non-zero entry in M_R^2 is also a non-zero in M_R.

[example in slide 9 pdf]

Transitive closure: adding all relative transitive pairs together.

2.9 Equivalence Relations

Equivalence Relation. iff it is reflexive, symmetric and transitive. I.e;

- For all $x \in A, x \sim x$;
- For all $x, y \in A, x \sim y$ implies $y \sim x$;
- For all $x, y, z \in A, x \sim y$ and $y \sim z$ implies $x \sim z$.

($\sim$: equivalent; equivalent under $\sim$; congruence modulo m is an equivalence relation)

[example in slide 10 pdf]

Equivalence class. Setting $\sim$ be an equivalence relation on set A; $a \in A$; equivalence class $[a]$:

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

set of all elements that are equivalent to a.

[example in slide 10 pdf]

Theorem: Set of equivalence classes of A under equivalence relation on A is a partition of A;
(i) A is the union of all the equivalence classes and
(ii) different equivalence classes are disjoint.

[proof + examples in slide 10 pdf]

Natural representative. finding the simplest member of each equivalence class. (could be smallest); set of natural representatives is **quotient set.**

[example in slide 10 pdf]

2.10 Partial Orders

Partial order iff it is reflexive, antisymmetric and transitive. I.e;

• For all $x \in A, x \sim x$;
• For all $x, y \in A, x \sim y$ and $y \sim x$ implies $x = y$;
• For all $x, y, z \in A, x \sim y$ and $y \sim z$ implies $x \sim z$.

$\preceq$: precedes; used to denote a partial order

For a, b where atleast $a \preceq b$ or $b \preceq a$, it is called total order.

[example in slide 11 pdf]

Posets. Posets (partially ordered sets) is a set A togehter with $\preceq$, denoted by $(A, \preceq)$. For poset $(A, \preceq)$
• If $a \preceq b$ then a is a predecessor of b.
• If $a \preceq b$ but $a \neq b$ (ie $a \prec b$) then we say a strictly precedes b.
• We say a is an immediate predecessor of b iff $a \prec b$ and there is no $c \in A$ such that $a \prec c \prec b$.
• Elements a, b are comparable if either $a \preceq b$ or $b \preceq a$. Otherwise, a, b are incomparable.

Set with total order is called totally ordered set (total order is partial order when any two elements are comparable).

[example in slide 11 pdf]

Hasse Diagrams. Small poset with directed graph:
• Elements of A are drawn as vertices.
• No loops drawn to indicate $a \preceq a$ (is already assumed).
• If $a \prec b$ then a is drawn longer than b (assume all arrow point upwards).
• If a is an immediate predecessor of b then upwards line is drawn from a to b.
• Any line that can be deduced from transitivity is omitted.

[example in slide 11 pdf]

Further definitions. Let $(A, \preceq)$ be a poset.
• Maximal: $a \in A$ if no $b \in A$ with $a \prec b$.
• Minimal: $a \in A$ if no $b \in A$ with $b \prec a$
• Greatest Element: $a \in A$ iff for all $b \in A, b \preceq a$.
• Least Element: $a \in A$ iff for all $b \in A, a \preceq b$.

Note. slight difference between greatest element and maximal element.

[example in slide 11 pdf]

Suppose $(A, \preceq)$ and $S \subseteq A$. Then:
• Upper Bound of S: $a \in A$ if $s \preceq a \forall s \in S$.
• Lower Bound of S: $a \in A$ if $a \preceq s \forall s \in S$.
• Least Upper Bound of S: $a \in A$ if it is an upper bound for S and for every otehr upper bound b of $S, a \preceq b$.
• Greatest Lower Bound of S: $a \in A$ if it is a lower bound for S and for every otehr lower bound b of $S, b \preceq a$.

[example in slide 11 pdf]

3 Logic and Proofs

3.1 Introduction to Logic and Proofs

Mathematical proof: consists of logical deduction on the basis of agreed premises. Apart from human error the results are certain.

Techniques for Proof:

• Always explain what you are doing, and your reasons for drawing your conclusions.
• Simplify!
• Keep the aim in mind.
• Plan a solution.
• Work on one side of an equation or inequation to relate it to the other.

To study proofs: you always have to practice!! No matter what. There are techniques, but most of the time you will have to practice proofs.
What we study is methods of proof and logic.

3.2 Example of Proofs

[in word?? mostly?? i think so yeah]

Example: $\frac{1}{1000} - \frac{1}{1001} < \frac{1}{1000000}$.
Techniques:
1. Common denominator (simple answer);
2. Reciprocals; 1/2a < 1/a kinda way (bigger denominator smaller fractions)
3. Simplify

Proof. We have

$$\frac{1}{1000} - \frac{1}{1001} = \frac{1001 - 1000}{1000 \text{ x } 1001} = \frac{1}{1001000}$$

But $1001000 > 1000000$, and both are positive numbers, so

$$\frac{1}{1001000} < \frac{1}{1000000}$$

Therefore

$$\frac{1}{1000} - \frac{1}{1001} < \frac{1}{1000000}.$$

It is handy to use calculators, but this is generally bad practice as there is no understanding.

Equality proofs should ideally not be proved by calculators!

3.3 Further Examples fo Proofs

Another example:
Example: $\sqrt[8]{8!} < \sqrt[9]{9!}$.
[rough working]

$$\Rightarrow 8! < \sqrt[9]{9!^8},$$
$$\Rightarrow (8!)^9 < (9!)^8,$$
$$\Rightarrow (1 \times 2 \times \cdots \times 8)^9 < (1 \times 2 \times \cdots \times 9)^8,$$
$$\Rightarrow (1 \times 2 \times \cdots \times 8)^9 < (1 \times 2 \times \cdots \times 8)^8 \times 9^8,$$
$$\Rightarrow 1 \times 2 \times \cdots \times 8 < 9^8.$$

which is obviously less than 9 times 9 times etc, therefore making the statement true.

However, you can't start like this. Ie, you have to start with the fact that is true, then ending up with the question.
You have to check if it can be reversed (ie reversing steps in a proof: is that possible?).
(in this case, you can reverse it: proof in word.)

Things to learn from this proof:

• Go back to definitions (expand the definition)
• Simplify!
• A proof is often discovered by working backwards; but it must often be written forwards.
• Explain logical and technical steps in words (with punctuation!)

3.4 Generalisation and 'All' Statements

• For examples such as $\frac{1}{1000} - \frac{1}{1001} < \frac{1}{1000^2}$, we can replace n with 1000 to give:

$$\frac{1}{n} - \frac{1}{n+1} < \frac{1}{n^2},$$

where $\forall n \in \mathbb{Z}^+; \frac{1}{n} - \frac{1}{n+1} < \frac{1}{n^2}$.

This is called a **universal statement** (an 'All' statement). The replacement of n with 1000 as such is called **generalisation**.
[proof for the n statement in word]

Things to learn:

• A common proof pattern for $\forall x \in A,$ property B holds is:

$$\text{Let } x \in A. \ldots \text{Therefore } x \text{ has a property } B.$$

• Cannot be proved by listing examples

All Statement Written in:
•$\forall x \in A,$ property B holds;
• For Each $x \in A, x \in B$;
• every A is a B;
• if x is an $A,$ then x is a B;
• No A is not a B;
•$\forall x \in A, x \in B$;
• B is true if A is true;
• A is true only if B is true;
• property A is sufficient(information) for property B to hold;
• property B is necessary for property A to hold;

[example in word]

3.5 Exhaustion of Cases

[proofs in word]

Things to learn from these sort of proofs:
• Explain what you are doing
• Outline proof like how you would outline 'all' statement Proofs
• Often useful where there is natural division of the problem into smaller cases (like where you can use induction or splitting into cases as such);
Examples include absolute value proofs, (modular) congruences or divisibility.
• Clearly state the seperate cases, and be sure all cases really are covered.
• Patterns for "if A then B" is:

Suppose that A is true ... Therefore B is true.

• Expand the definition
• Keep aim in mind!!! Find general steps, substitute, reduce where necessary.

3.6 Writing Proofs

[proofs in word] • Usually involves two stage:
1. Discover reasons why statement is true
2. present these reasons as a coherent, carefully written argument.

Theorem 1. *Let n be an integer. If n is even, then n^2 is even.*
• *use a basic idea to prove it (for example, $n = 2k$, so $n^2 = 4k^2$).*

Things to learn from proof
• Written in complete sentences, with correct spelling and grammar!
• Sentence should begin with a word, not a variable/number.
• In text, writing equations consequtively with no words between them can make it unclear.

Bad Practice: Let $n = 2k, k \in \mathbb{Z}$.

Good practice: Let $n = 2k,$ where $k \in \mathbb{Z}$.

Structure of a Proof
• Begin with a clear statement.
• Write the word "Proof"; then begin argument.
• Any notation used; introduce variables properly.
• Logic of the proof should be clear.
• Include a conclusion that indicates end. Can include "QED" but not necessary.

Helping the reader
• Give reasons for all conclusions.
• Helpful to explain technical and algebraic steps.
• Need to make comments about variables being integers, etc.
• Try to the get the level of the argument right.

3.7 Converse; If and Only if

The **converse** of "if A then B" is "if B then A", and so forth.

Converse of a statement may or may not be true.

Converse fallacy refers to try and prove the converse of the statement because it is not true.

[examples in word]

Things to Learn from the proof

• Disproving an "all" statement just means finding a counterexample; ie find one example where A is true but B is false.

If and only if When a statement "if A then B" and converse "if B then A" are both true, then we can combine it to write "A iff B" ($A \leftrightarrow B$).

Statement can be rephrased as the following:
• "if A then B", conversely "every A is B and every B is A".
• A is a necessary and sufficient condition for B;
•$A \iff B$.

[examples in word]

Note: "Iff" statements really consists of two statements; therefore proof is of two parts.

Common proof patter for iff statements:
"Firstly, let x be an A" ..."Therefore, x is a B." "Conversely, let x be a B. ... Therefore, x is an A.

Theorem 2. *Let $n \in \mathbb{Z}$. Then, $6|n$ iff both $2|n$ and $3|n$.*

(1. suppose $6|n$, then find $2|n$ and $3|n$; then prove converse [converse; $\gcd(2,3) = 1$ therefore $2 \times 3|n$].)

Things to learn from proof:
• Expand definitions!!
• Keep goal in mind.
• Make logical subdivision clear by writing "Firstly" and "Conversely"
• Each part follows the normal format for an "if ... then" proof.
• "Similarily" saves work for the reader, not the writer.

3.8 "Some" Statements

Asserts that there exists something which satisfies a certain condition.

"There exists something such that ..." means that there is one object or more with the given property.

For example: "there exists $x \in \mathbb{R}$ such that $x^2 = 2$"

Examples of "some" statements

- Some integers are positive.
- There exists a function $f : \mathbb{R} \to \mathbb{R}$ which is both odd and even.
- Some students enjoy doing Maple tests.
- $S \neq \emptyset$.
- $6|n$.
- a is odd.

A "some" statement can be written as:

- some A is a B;
- some As are Bs;
- there exists an A which is (also) a B;
- for some $x \in A$ we have $x \in B$;
- property B holds for some $x \in A$;
- $\exists\ x \in A : x \in B$;

[example in word]

Things to learn from proofs:

- Discover the proof by working backwards; but write proof in right order.
- Real work is "behind the scenes"; requires much more knowledge of algebra and calculus.
- Proof with f gives a "some" statement which has an "all" statement within.

3.9 "Some" statements confused

Sometimes it is possible to prove a "some" statement without producing any particular object.

Example: Let $f(x) = x^5 + 2x - 2$. Then $f(x) = 0$ for some $x \in [0, 1]$.
Check end points. The graphs are continuous curves.

Proof. Let $f(x) = x^5 + 2x - 2$. Then, $f(0) = -2$, which is negative, while $f(1) = 1$; which is positive. So, the graph of f, being a continuous curve, must cross x-axis somewhere between 0 and 1; and at this crossing point we have $f(x) = 0$.
(existence proof) therefore, it completes the proof.

[other example in word]

Things to learn from proofs:

• Needed background knowledge
• Tedious to find actual x and y values to prove, so find generic solutions that make proofs easier.
• "Clearly" does not mean you don't have to check the following statement. (ie you have to check if the most obvious statement in the question is also true.)

Existence and uniqueness. A statement of the form "there exists a unique $x \in S$ such that ..."
asserts that there is one and only one object having the given property.

Proof for such statements:
• show $\exists$ an object with given property;
• show there cannot be two diff objects with property. Common proof patter is as follows:

"Suppose that x_1 and x_2 have the same property."
...
"Therefore, $x_1 = x_2$."

[examples in word: $a = bq + r$.]

Things to learn from proof:
• Clearly distinguish the "existence" and "uniqueness" parts of the proof.

3.10 Multiple Quantifiers

• The words "all" and "some" -¿ quantifiers. A statement can have more than one quantifier.

Examples:
• For every $x \in \mathbb{Z}, \exists y \in \mathbb{Z}$ such that $y > x$.
• $\exists y \in \mathbb{Z}$ such that for every $x \in \mathbb{Z}, y > x$. (not the same as the first statement.)
• $2^29 - 1$ is composite. (rewrite: $2^29 - 1 = ab$ where $a > 1, b > 1$ for some integers a, b.)
• For any prime there is a larger prime.
• $(6, -1, 5)$ is a linear combination of $(1, 1, 2)$ and $(1, 2, 3)$.
• There is a function $f : \mathbb{R} \to \mathbb{R}$ which is equal to its own derivative.
• Every positive real number has a real square root.
• For all $A, B, C \subseteq U, A \cup (B \cup C) = (A \cup B) \cup C$.
• The function $f : X \to Y$ is onto.

Theorem 3. *Any composite positive integer has a factor greater than* 1 *and less than or equal to its square root.*

Note: Making the quantifiers explicit, the statement is:

"for every composite integer n $\exists$ c, a factor of n such that $c > 1$ and $c \leq \sqrt{n}$".

Let n be composite.

$$n = ab, a > 1, b > 1.$$

Case $I : a \leq \sqrt{(n)}$

$$c = a, \text{ has required properties.}$$

Case $II : a > \sqrt{n}$

$$c = b; b = \frac{n}{a} < \frac{n}{\sqrt{n}} = \sqrt{n}.$$

Therefore, $c|n, 1 < c \leq \sqrt{n}$.

Things to learn from proof:
• Rewrite the given statement if necessary to make the quantifiers clear.
• Patter of "all" proof: within this, patter of "existence" proof.
• Another example of "proof by exhaustion" of cases.
• Expand the defintion!!

3.11 Multiple quantifiers continued (limits)

Theorem 4. $\lim_{x\to\infty} \frac{4x^2+7x+19}{2x^2+3} = 2$.

Note: According to definition of a limit, we must show that for every $\epsilon > 0, \exists$ a real number M such that

$$\text{if } x > M \text{ then } | \frac{4x^2+7x+19}{2x^2+3} - 2 | < \epsilon.$$

Proof: Let $x > 0$.
Choose $M = \max(1, \frac{10}{\epsilon})$.
Let $x > M$. Then

$$x > 1 \text{ and } x > \frac{10}{\epsilon}.$$

so

$$\begin{aligned} | \frac{4x^2+7x+19}{2x^2+3} - 2 | &= | \frac{7x+13}{2x^2+3} |, \\ &= \frac{7x+13}{2x^2+3}, \\ &< \frac{7x+13}{2x^2} \text{ (because } x > 1), \\ &= \frac{10}{x}, \\ &= \frac{10}{\frac{10}{\epsilon}} \text{ (since } x = \frac{10}{\epsilon}), \\ &= \epsilon. \end{aligned}$$

Therefore, $\lim_{x\to\infty} \frac{4x^2+7x+19}{2x^2+3} = 2$.

Things to learn from proof:
• Expand definition!!
• Logical structure of statement to be proved is: "for all ... there exists ... such that if ... then ...", and proof follows structure properly.
• Working backwards is very important!!

3.12 Change of order of quantifiers

Two adjacent quantifiers of the same kind can be interchanged. Example:

$$\exists\ \alpha \in \mathbb{R}, \exists\ \beta \in \mathbb{R}, (6, -1, 5) = \alpha(1, 1, 2) + \beta(1, 2, 3).$$

means the same as:

$$\exists\ \beta \in \mathbb{R}, \exists\ \alpha \in \mathbb{R}, (6, -1, 5) = \alpha(1, 1, 2) + \beta(1, 2, 3).$$

as both statements exert two variables being real numbers; satifies equation.

Another example:

$$\forall A \subseteq U, \forall B \subseteq U, A \cap B = B \cap A.$$

and

$$\forall B \subseteq U, \forall A \subseteq U, A \cap B = B \cap A.$$

are the same as it is both subsets of U.

"All" and a "some" quantifier may not be interchanged.

[example in word]

Things to learn from proof:
- Clearly distinguish between what is given and what you have to prove
- "imaginative" step of the proof: come up with 'numbers' to suit the equation.
- Working backwards is important
- Going back to the definition is a profitable idea.

3.13 "Not" and contradiction

Negation of statement -¿ asserts that the statement is false.

Notation: $\sim A$, $\neg A$ or $\sim (A)$.

Examples
• Negation of $2+2=5$ is "it is false that $2+2=5$" or $2+2 \neq 5$.
• Negation of $\frac{1}{n} - \frac{1}{n+1} < \frac{1}{n^2}$ is $\frac{1}{n} - \frac{1}{n+1} \geq \frac{1}{n^2}$.
• However, $A \subset B$ is not $A >= B$! it is $A \not\subseteq B$.

[example in word]

Things to learn from proof:
• This proof is called **proof by contradiction** or reductio ad absurdum.
• Deciding statement true or false: work out consequeunces till u find something that is known to be true or false.

Distinguish formats of **proof by contradiction** .
1. "Suppose A is true. ... Therefore B. But B is false. Therefore A is false. " -¿ **VALID** reasoning.
2. "Suppose A is true. ... Therefore B. But B is true. Therefore A is true. " -¿ **INVALID** reasoning (dont use this if using proof by contradiction).

[example in word]

Things to learn from proof:
• Proof by contradiction begins with assuming negation of statemetn to be proved.
• Be extremely careful with logic and setting out of a proof by contradiction.
• Make proof easier to read by introducing suitable notation.
• Essentially "sub-proof" by contradiction within the main proof by contradiction.
• Justifiable use of the word "similarily".

3.14 Contrapositive

Contrapositive of a statement "if A then B" is "if not B then not A".

• Another example: "every A is a B" is "anything which is not a B is not an A".

Logically equivalent to the original.

Possible proof pattern:
" Suppose B is false ... then A is false. Therefore, by Contrapositive, A and B would be true."

Examples
• Let $f : X \to Y$.. Contrapositive of "if $x_1 \neq x_2$, then $f(x_1) \neq f(x+2)$" is "if $f(x_1) = f(x_2)$ then $x_1 = x_2$."
• Contrapositive of "if n^2 is ever, n is even" is "if n is odd, n^2 is odd".
[other examples in word]

Things to learn from proof:
• Contrapositive is valuable and gives more direct information than trying to prove the statement itself.
• If you're using contrapositive, it is a good idea to say so in the beginning.
• substitute "if ... then" proof.

[other example in word: $\sqrt{2}$ is rational]

Things to learn from the proof:
• As for reductio ad absurdum, proof begins by assuming given statement is false.
• Proving a number is irrational nearly always involve proof by contradiction.

3.15 More examples of negation and negation of

More examples of negation:

• The negation of "all first-year maths is easy" is "not all first-year maths is easy".
• Negation of "there exists $x \in \mathbb{R}$ such that $x^2 = -1$." is "there does exists $x \in \mathbb{R}$ such that $x^2 = -1$." or "for all $x \in \mathbb{R}, x^2 \neq -1$".
• Negation of "for all $x \in U$" is "for some $x \in U$, not $(\dots)$".
• Negation of "for some $x \in U$" is "for all $x \in U$, not $(\dots)$".

[write a counterexample to disprove all statements and for "some" statements, can prove "all" statement or proof by contradiction.]

[example in word]

Things to learn from this proof:

• Try a few examples if the proof is not so obvious. This either proves a counterexample or gives a pattern that you can work with later.

Negation of multiple quantifiers The above equivalences can be used repeatedly to simplify the negation of statement containing multiple quantifiers.

Example Simplify the negation of:

$$\forall x \forall y \exists z \dots .$$

Solution The negation is:

$$\sim (\forall x \forall y \exists z \dots),$$

that is,

$$\exists x \sim (\forall y \exists z \dots),$$

or

$$\exists x \exists y \sim (\exists z \dots),$$

or finally,

$$\exists x \exists y \forall z \sim (\dots).$$

[another example (calc) in word]

Things learned from the proof:
• Draw pictures to assist intuition.
• Negation of "if A then B" can be expressed as "A and not B".
• First three lines of the proof deal (in correct order) with the three quantifiers in the statement to be proved.

3.16 Mathematical induction 1

Mathematical induction is useful for proving "all" statements, specially about natural numbers.

Mathematical induction of the statement "for all $n \in \mathbb{N}$ consists of two parts:
1) prove ... for $n = 0$;
2) prove that if ... is true for some value $k \in \mathbb{N}$ then ... is true for $k + 1$.

Likewise, "for all $n \geq n_0, \ldots$" can be proved by mathematical induction by:
1) prove ... for $n = n_0$:
2) prove that if ... is true for some particular value of $n \geq n_0$, then it is true for $n + 1$.

Step 1) is called the **basis** of proof; Step 2) is called the **inductive step**.

[proof in word]

Things to learn from proof:
• Inductive proof format:
"Let $n = 1$ ... Therefore result is true for $n = 1$. Now assume that the result is true for some particular n. We must prove that ... Therefore result is true for $n + 1$. By induction, the result is true for all $n \geq 1$."
• To make induction work, we need some simple relation between n and $n + 1$.

[proof in word]

Things learnt from proof:
• Never multiply an inequality by anything unless you are sure that the "anything" (number which is multiplied in this case) is positive or negative.

3.17 Mathematical Induction 2

Strong induction or extended induction

Suppose statement true for $n = 0$ and $n = 1$; and if is true for consecutive integers n and $n + 1$, then it is true for $n \geq 0$.

[example in word]

Things to learn from proof:
• Here, proof depends upon knowing if it holds true for the previous two values. That is why, always prove for the first two values when this is the case.
• Keep aim in mind!
• Usually used for recurrence relations.
• In case like this, be absolutely clear on what is given and what is required to prove.
Extend the method even further; suppose:
(i) a certain statement is true for $n = 1$;
(ii) for any particular $n \geq 1$, if the statement is true for $1, 2, 3, \ldots n$ then it is true for $n + 1$.
Then, the statement is true for all $n \geq 1$.

[example in word]

3.18 Logic

Logic is the study of how the truth or falsity of a given statement follows (or not!) from the truth of other statements. For example, given the statements

"if G is an Eulerian graph, then no vertex of G has odd degree" and "G is an Eulerian graph",

we may conclude with "no vertex of G has odd degree".

Note. The logic we have used here says nothing about whether the first two statements are actually true or not, but only that if they are true, then the third is also.

Definition. A proposition is a statement which is unambiguosly true or false.

Examples.

• $1 + 1 = 2$;
• $2 + 2 = 3$;
• my birthday is on 29 February;
• there exist infinitely many primes p for which $2^p - 1$ is also prime. (mersenne primes)

Not proposition example: $2 + 2$, etc.

Complicated expressions use logical operators such as:
• "not": $\sim$;
• "and": $\wedge$;
• "or": $\vee$;
• "exclusive or": $\oplus$;
• "if . . . then": $\rightarrow$;
• "if and only if": $\leftrightarrow$.

Examples. if p, q, r are propositions:

• $p \wedge (\sim q)$ means "p and not q";
• $(\sim q) \rightarrow (\sim p)$ is the contrapositive of $p \rightarrow q$;
• $q \rightarrow p$ is the converse of $p \rightarrow q$.
These are called "propositional forms".

[example in 3*b* pdf]

3.19 Truth Tables

Logic of propositions: give **truth** values T or F for propositions $p, q, r, \ldots$ and determine the truth value for a certain commpound composition.

[truth value tables in 3b pdf]

•"And": conjunction;
•"Or": disjunction (inclusive meaning of or).

[example in 3b pdf]

Definition. Two proposition forms are logically equivalent if they have the same truth values for each possible allocation of truth values to variables in them.
Denote logical equivalence of P and Q by writing $P \Longleftrightarrow Q$.

De Morgan's Law. $\sim (p \vee q) \Longleftrightarrow (\sim p) \wedge (\sim q)$.

[example in word]

If RHS and LHS for particular statements have same truth values in all cases, then $p \wedge (q \vee r) \Longleftrightarrow (p \wedge q) \vee (p \wedge r)$. which is **Distributive Law** .

Defition.
• Propositional form that is always true is called "tautology".
• Proposition form that is always false is called "contradiction".
• Proposition that is neither a tautology or a contradiction is called "contigency".

Example
• $p \vee (\sim p)$ is tautology.
• $p \wedge (\sim p)$ is contradiction.
• $p \wedge q$ is a contigency.

Note.

1) Any two tautologies/contradictions are logically equivalent, as they have same truth value for all cases.
2) Conversely, if a proposition is equivalent to a tautology, then the proposition itself is a tautology.

3.20 Laws of logical equivalence

Laws of logical equivalence. let p, q, r be propositional variables, let T be tautology and F a contradiction. Then:

$$\sim (p \vee q) \iff (\sim p) \wedge (\sim q),$$

$$p \wedge (q \vee r) \iff (p \wedge q) \vee (p \wedge r),$$

$$p \vee (\sim p) \iff T, (1)$$

$$p \wedge (\sim p) \iff F, (2)$$

$$\sim (p \vee q) \iff (\sim p) \wedge (\sim q) \text{ and } \overline{A \cup B} = \bar{A} \cap \bar{B},$$

$$p \vee (\sim p) \iff T \text{ and } A \cup \bar{A} = \mathcal{U},$$

$$p \wedge (\sim p) \iff F \text{ and } A \cap \bar{A} = \emptyset.$$

Note. (1) and (2) are dual pairs of logical equivalences.

Laws. (most useful logical equivalences)
• Commutative Law:

$$p \wedge q \iff q \wedge p \text{ and } p \vee q \iff q \vee p,$$

• Associative Law:

$$(p \wedge q) \wedge r \iff p \wedge (q \wedge r) \text{ and } (p \vee q) \vee r \iff p \vee (q \vee r),$$

• Distributive Law:

$$p \wedge (q \vee r) \iff (p \wedge q) \vee (q \wedge r) \text{ and } p \vee (q \wedge r) \iff (p \vee q) \wedge (q \vee r),$$

• Identity laws:

$$p \wedge T \iff p \text{ and } p \vee F \iff p,$$

• Laws of negation:

$$p \vee (\sim p) \iff T \text{ and } p \wedge (\sim p) \iff F,$$

• Double negation law:

$$\sim (\sim p) \iff p,$$

• Idempotent Laws:

$$p \wedge p \iff p \text{ and } p \vee p \iff p,$$

• Domination Law:

$$p \vee T \iff T \text{ and } p \wedge F \iff F,$$

• De Morgan's Law:

$$\sim (p \wedge q) \iff (\sim p) \vee (\sim q) \text{ and } \sim (p \vee q) \iff (\sim p) \wedge (\sim q).$$

[example in pdf 3b]

If . . . then. $p \to q$. or "p implies q" or "if p then q". (always true except when p is true and q is false).

[truth table for logical equivalence involving $\to$ in pdf 3b + example]

Note. Non-equivalence of two propositional forms would normally be very difficult to prove by "algebraic" methods.

If and only if. Biconditional proposition $p \longleftrightarrow q$ is true when p and q are both true or both false, and is false otherwise (like when one is true and one is false, $p \longleftrightarrow q$ is false).

$$p \longleftrightarrow q \iff (p \to q) \wedge (q \to p).$$

• $p \iff q$ tells something about the two propositional forms;
• $p \longleftrightarrow q$ is a combination of the two propositional forms into a single form.

[theorem in 3b pdf + proof (for logical equivalence of two forms if and only if the forms in $\longleftrightarrow$ is a tautology.)]

Definition. Let P, Q be propositional forms. If P is true, Q is true. Then we can say P logically implies Q leading to $P \Longrightarrow Q$.

[example in 3b pdf]

3.21 Valid and Invalid arguments

Argument: "If G is an Eulerian graph, then no vertex of G has odd degree. G is an Eulerian graph. Therefore, no vertex of G has odd degree." is made using the rule of inference.
$p \to q$
p
$\therefore \bar{q}$.
(q is just the result. yeah)

Such an argument is always valid because the conclusion must always be true, provided hypotheses(earlier statements) are true.

This rule of inference is aclled "modus ponens".

Invalid inference example:
$p \to q$
p
$\therefore \overline{p}$.

Since some cases can be true and some can be false.

Note. Conclusion of a valid argument need not always be true. (for a true conclusion, we need a valid argument and true hypotheses).

Modus Tollens:
$p \to q$
$\sim q$
$\therefore \overline{\sim p}$.

[truth tables of modus ponens in 3b pdf]

Theorem 5. *An argument $P_1 P_2 \dots P_n \overline{Q}$ is valid if and only if $(P_1 \wedge \_2 \wedge \dots \wedge P_n) \Longrightarrow Q$ that is, if and only if the proposition $(P_1 \wedge \_2 \wedge \dots \wedge P_n) \longrightarrow Q$ is a tautology.*

[proof in 3b pdf]

Things to learn from proof:
• Structure of an "if and only if" proof.
• Proof by division into cases.
• Proof by contrapositive.

[example in word]

Theorem 6. *The rule of inference:* $(\sim p) \longrightarrow F \therefore p$. *is valid.*

[proof in 3b pdf; formal verification of method by proof of contradiction]

[problem in 3b pdf + solution]

4 Combinatorics

4.1 Brief Introduction 1

- basically doing counting, with different techniques and such;
- Formulise all techniques taught and apply it to real world as such.

4.2 Addition and Multiplication Principles

Proposition: Addition Principle

Let $A_1, \dots A_n$ be finite sets so that $A_i \cap A_j =$ for $i \neq j$.
Then, $— A_1 \cup \cdots \cup A_n — \; = \; — A_1 — \; + \cdots + \; — A_n —$.

Proposition: Multiplication Principle:
Let $A_1, \dots, A_n$ be finite sets. Then,
$— A_1 \times \cdots \times A_n — \; = \; — A — \; \dots \; — A_n —$.

• Addition Principle: can be used for questions such as 'how many choices in total? -¿ add to total', etc and
• Multiplication Principle can be used for questions such as "choose one from the others -¿ total possible combinations"

Example: A restaurant menu has 7 mains and 3 desserts.

a) If one has to choose a main or a desert (but not both), how many choices would one have?

$A_1 =$ choices of mains , $A_2 =$ choices of desserts .
$— A_1 \cup A_2 — \; = \; — A_1 — \; + \; — A_2 — \; - \; — A_1 \cap A_2 —$,
$— A_1 \cup A_2 — \; = \; — A_1 — \; + \; — A_2$ since $— A_1 \cap A_2 — \; =$,
$— A_1 \cup A_2 — \; = 7 + 3 = 10.$

b) If one was to choose one main and dessert, how many choices does one have?

$A_1 =$ choices of mains , $A_2 =$ choices of desserts .
Asking $— A_1 \times A_2 — \; = \; — A_1 — x — A_2 —$,
$— A_1 \times A_2 — \; = 7 \times 3 = 21.$

4.3 A remark on the addition principle

Example:
Last year, 431 students enrolled in MATH1081 and 562 students enrolled in MATH1131. How many students enrolled in either courses?

A) We can't tell! Not enough information about number of students enrolled in both courses.
If $A_1 =$ students in MATH1081, $A_2 =$ students enrolled in MATH1131,

It is not clear that $A_1 \cap A_2 =$, so the addition principle does not apply.

4.4 Warm-up example words in alphabet

Example:
1. How many 3 letter words are there in an alphabet?

A) (Choices for letter 1): 26× (Choices for letter two): 26× (Choices for letter three): $26 = 26^3$.

2. How many 3 letter workds contain exactly one vowel?

A) Choices for letter one times choices for letter two times choices for letter 3 but with 3 cases, where:
(*i*) vowel position 1: $5 \times 21 \times 21$.
(*ii*) vowel position 2: $21 \times 5 \times 21$.
(*iii*) vowel position 3: $21 \times 21 \times 5$.
Total $= 5 \times 21 \times 21 + 21 \times 5 \times 21 + 21 \times 21 \times 5$,
$= 3 \times 5 \times 21 \times 21$. (where it could be (number of combinations) times (number of words with one vowel); if all the combinations are the same).

3. How many 3 letter words come before 'EGG' in alphabetical order?

A) 3 ways to do so:

(*i*) First letter is A, B, C or D.
(*ii*) First letter is E and second letter is A, B, C, D, E or F.
(*iii*) First letter E, second G, and third letter is A, B, C, D, E or F.

(*i*) $= 4 \times 26 \times 26$
(*i*) $= 1 \times 6 \times 26$
(*i*) $= 1 \times 1 \times 6$
Total $= (4 \times 26 \times 26) + (1 \times 6 \times 26) + (1 \times 1 \times 6)$,

4.5 Ordered selection with repetition

Example: 1. How many 3 letter words are there in an alphabet?

A three letter word can be thought of as a function: $w : \{1, 2, 3\} \to \{A, B, C, \ldots, Z\}$.
where $w(i) =$ letter in i^{th} position.

Theorem 7. *Ordered Selection with repetition: Given two finite sets N and M whose coordinates are: $-N- = n$ and $-M- = m$,*
Number of functions $f : N \to M$ is given by: Fun $(N, M) = m^n$.

Note. secretly think of N as the set of positions of selection $\{1, 2, 3, \ldots, n\}$.

Proof. Let elements of N be called $N = \{1, 2, 3, \ldots, n\}$.

Given $m := (m_1, \ldots m_n) \in M \times M \times \cdots \times M$.
Define $f_{\underline{m}} : N \to M$ by $f_{\underline{m}} : i \to m_i$.
Gives a function of $g : M \times M \times \cdots \times M \to$ Fun (N, M); $g : \underline{m} \to f_{\underline{m}}$.

Note for $f \in$ Fun (N, M) define $\underline{b}_f := (f(1), f(2), \ldots, f(n)) \in M \times M \times \cdots \times M(n$ times $)$,
This gives a function $h :$ Fun $(N, M) \to M \times M \times \cdots \times M$.
Now (check) $h \circ g = id_{M \times M \times \cdots \times M}$ and $g \circ h = id_{M \times M \times \cdots \times M}$,

so h is a bijection with inverse g.

Therefore, $-$ Fun $(N, M) - = -M \times M \times \cdots \times M - = m^n$, (by defition of multiplication principle).

4.6 Ordered selection without repetition

Example.
How many four letter words in the letter A, B, C, D can be made with each letter appearing atmost once?

A) Choices for first letter: 4
Choices for second letter: 3
Choices for third letter: 2
Choices for fourth letter: 1
Total $= 4 \times 3 \times 2 \times 1$.

Alternatively, we can think of the function as $w : \{1, 2, 3, 4\} \to \{A, B, C, D\}$, $i \to$ letter in the ith position , the added restriction translates into the condition that is w is bijective.

Theorem 8. *Rearranging distinct objects: Given finite set N so that: $— N — = n$, the number of bijections $f : N \to N$ is given by $— Bij(N, N) — = n!$.*

Proof. Follows from a theorem that is to come (skip for now.)

Example. How many injections are there from $\{1, 2\} \to \{A, B, \ldots, Z\}$?

A) Asking for two letter words with one letter appearing more than once.
Choices for first letter: 26
Choices for first letter: 25
Total $= 26 \times 25$

Theorem 9. *Ordered selection without repetition: Let R and N be finite sets so that $— R — = r$, $— N — = n$ and $r \leq n$.*
Number of injections: $f : R \to N$ is given by $— Inj(R, N) — = \frac{n!}{(n+1)!}$

Note. Convention $0! = 1$.

Notation. We use $P(n, r)$ to denote the number

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

$(n - r)! =$ first r terms.

Proof of Ordered selection without repetition.
By induction on $— N — , f — N — = 1$, then $— R — = 1$ and $— \text{Inj}(R, N) — = 1$.

Assume result is true for $— N — = K$ and consider the case $— N — = K + 1$.
Note the result depends on sizes of R and N so assume $R = \{1, 2, 3\}, r \leq k + 1, N = \{x_1, x_2, \ldots, x_{k+1}\}$.

$$S = \text{Inj}(R, N) = \{f : R \to N — f \text{ is injective}\}.$$

Consider subsets: $S_i := \{f \in S — f(i) = x_{k+1}\}, S_{x_{k+1}} := \{f \in S — f(i) \neq x_{k+1} \forall i \in \mathbb{R}\}$.

Observe. $S = S_1 \cup S_2 \cup \cdots \cup S_{x_{k+1}}, S_i \cap S_j =$ for $i \neq j$ and $S_i \cap S_{x_{k+1}} =$. (injective)
Therefore, by addition principle,

$$\boxed{— S — = — S_1 — + — S_2 — + \cdots + — S_r — + — S_{x_{k+1}} —}$$

Now, compute S_i. (bijective to $\{f : R - \{i\} \to N - \{x_{k+1}\}\}$), inductions hypothesis $— S_i — = \frac{K!}{(K-(r-1))!}$. ($— N - x_{k+1} — = K$.)

Note bijection of $— S_{x_{k+1}} —$ bijection with injective $f; \{f : R \to N - x_{k+1}\}$ but $— N - x_{k+1} — = K$ so induction hypothesis gives $— S_{x_{k+1}} — = \frac{K!}{(K-r)}!$

Putting everything together:

$$\begin{aligned} — S — = — S_1 — + — S_2 — + \cdots + — S_r — + — S_{x_{k+1}} —, \\ = r\frac{K!}{(K-(r-1))!} + \frac{K!}{(K-r)!}, \\ = \frac{K!(K+1)}{((K+1)-r)!} = \frac{(K+1)!}{((K+1)-r)!}. \end{aligned}$$

4.7 Example ordered selection without repetition

Example. A group fo 13 pirates are to take a team photo. Photogrpaher asks them to organise so that 6 of them sit in a row of seats while the other 7 stand behind them. If we do not order who sits on which seat, how many different arrangements are there?

A) Choices for seat 1: 13
Choices for seat 2: 12
...
Choices for seat 6: 7
Total = $P(13, 6) = \frac{13!}{6!}$

*Q*2)If the chief and his second in charge must sit in the middle two seats, how many different arrangements are there?

A) Choices for seat 1: 11
Choices for seat 2: 10
Choices for seat 3: 2
Choices for seat 4: 1
Choices for seat 5: 9
Choices for seat 6: 8
Total = $2 \times P(11, 4) = 2 \times \frac{11!}{4!}$.

4.8 Remark challenging counting problems

Example. For a number n a partition is a set of numbers $a, \ldots, a_k$ so that $a_1 + a_2 + \cdots + a_n = n$. (ie $4 = 4 = 3 + 1 = 2 + 2 = 2 + 2 + 1 \ldots$; 5 partitions.) What is the number of partitions in 557?

A) find a pattern and then you can get the number of partitions for 557.

4.9 Examples counting up to symmetries

Example. How many words can you make by rearranging the letters in the word "MOON"?

A) First, distinguish that there are two "O"s in "MOON". There are 4! such rearrangements but they come in pairs. (swap one O with the other O).
MO_1NO_2 then MO_2NO_1.
Therefore, if we were to disregard the difference between O_1 and O_2, then we get $\frac{4!}{2!}$.

Example. How many words can be made by rearranging the letters in "CHEESE"?

A) Find there are 3 "E"s in "$CHE_1E_2SE_3$".
We have 6! words. But be careful that there can be combinations such as $CHE_1E_2SE_3 \sim CHE_2E_1SE_3$ and etc.

Note.
• the relation $\sim$ on the artificial words is an equivalence relation.
• Elements in any given equivalence class are in one-to-one correspondence with bijectors $f : \{E_1, E_2, E_3\} \to \{E_1, E_2, E_3\}$, so each equivalence class contains elements.

Therefore, number of rearrangements of "CHEESE" is $\frac{6!}{3!}$.

4.10 Unordered selection without repetition

Theorem 10. *Unordered selection without repetition: Given a finite set* $— N — = n$ *and an integer* r *with* $0 \leq r \leq n$*, the number of subsets* $R \subset N$ *so that* $— R — = r$ *is given by:*

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

where $\binom{n}{r}$ *is known as* n *choose* r*.*

Proof. Take R to be a set so that $— R — = r$.
Consider $S := \{f : R \to S — f \text{ is injective}\}$ and define a relation $\sim$ on S:

$$f \sim g \text{ iff } \text{image}(f) = \text{image}(g).$$

(i) Note $\sim$ is an equivalence relation
(ii) {equiv classes of $\sim \to$ subsets of $N$of size r}

$$f : R \to S \to \text{image}(f)$$

is bijective.
(iii) $f \sim g$ iff there is a unique bijection $h : R \to R$ so that $f \circ h = g$.

$$\text{Subset of} N \text{of size} r = \frac{\neq \text{injections } R \to S}{\neq \text{bijections } R \to S} = \frac{n!}{(n-r)!r!}.$$

4.11 Examples unordered selection without repetition

Remark. Counting subsets of a finite set is counting number of unordered elements in the same subset.

Example. How many 13 card hands have exactly 7 of one suit and 6 of another?
A) = Choices of suits to pick for 7 cards $\times$ Choices of 7 unordedred cards in a given suit $\times$ choices fo suits to pick six cards from $\times$ choices of 6 unordered cards in a given suit.

$$= 4 \times \binom{13}{7} \times 3 \times \binom{13}{6}.$$

Example. How many 13 card hands contain 4 cards in each of the two suits and 5 in another?
A) Choices of suits to pick 5 cards from $\times$ number of 5 cards in a given suit $\times$ choices of suits to pick 4 cards from $\times$ pick four cards from one of the suits $\times$ pick four cards from the other suit

$$= 4 \times \binom{13}{5} \times \binom{3}{2} \times \binom{13}{4} \times \binom{13}{4}.$$

4.12 Binomial theorem

Theorem 11. *let n be a non negative integer. Then,*

$$(x+y)^n = \sum_{r=0}^{n} \binom{n}{r} x^r y^{n-r}.$$

Proof. (idea)

$$(x+y)^n = (x+y) \times \cdots \times (x+y)(n\text{times}).$$

Only way to obtain a term $x^r y^{n-r}$ is to choose x coming from r of these factors.

Corresponds to choosing a subset of size r in a set of size n. Therefore, number of such terms in this expression is $\binom{n}{r}$.

4.13 Properties of binomial coefficients

(*i*) **Proposition.** Let r and n be in integers so $0 \leq r \leq n$. So:

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

(*ii*) **Proposition.** Let r and n be in integers so $1 \leq r \leq n+1$. So:

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

known as pascal's triangle. **Proof.**

$$\begin{aligned}
\binom{n}{r} + \binom{n}{r-1} &= \frac{n!}{(n-(r-1))!(r-1)!} + \frac{n!}{(n-r)!r!}, \\
&= \frac{n!r}{(n-(r-1))!r!} + \frac{n!(n-(r-1))}{(n-(r-1)!r!)}, \\
&= \frac{n!(r+n-r+1)}{((n-1)-r)!r!} = \frac{n!(n+1)}{((n+1)-r)!r!}, \\
&= \binom{n+1}{r}.
\end{aligned}$$

4.14 Another example of unordered selection without repetition

Example. How many length 8 biy strings contain at least 6 ones? *i*) How many such string contain exactly 6 ones?

$$\binom{8}{6}.$$

ii) How many such string contain exactly 7 ones?

$$\binom{8}{7}.$$

iii) How many such string contain exactly 8 ones?

$$\binom{8}{8}.$$

Strings with at least 6 ones = $\binom{8}{6} + \binom{8}{7} + \binom{8}{8}$.

The equivalent is to asking how many b8 bit strings contain at most 2 zeroes.
i) How many such string contain 2 zeroes?

$$\binom{8}{2}.$$

ii) How many such string contain 1 zeroes?

$$\binom{8}{1}.$$

iii) How many such string contain no zeroes?

$$\binom{8}{0}.$$

Strings with at most 2 zeroes = $\binom{8}{2} + \binom{8}{1} + \binom{8}{0}$.

4.15 Integer solutions to summation equation

Example. If Tony went to buy 4 scoops of ice cream, in which the flavours available are pistachio, chocolate and salted caramel, if Tarig would like to try each flavour, how many possible combinations are there?

A) Same as asking number of solutions to $x_1 + x_2 + x_3 = 4, x_i \in \mathbb{N} \cup \{0\}$.
Assume $x \geq 1$. Equivalent of asking how many ways we can group 4 ice creams into 3 groups. Doing so, we get $2 + 1 + 1 = 4$; given by $\binom{4-1}{3-1} = \binom{3}{2}$; where 3 is gaps between sticks and 2 is dividers required.

Theorem 12. *Let $r \leq n$ be positive integers. Then, the number of positive integers (0 not included) solutions of*

$$x_1 + x_2 + \cdots + x_r = n,$$

is given by $\binom{n-1}{r-1}$.

(proof in topic 4 pdf)

Theorem 13. *Let $r \leq n$ be positive integers. Then, the number of non negative integers (0 included) solutions to*

$$y_1 + y_2 + \cdots + y_r = n,$$

is $\binom{n+r-1}{r-1}$.

Proof. Define $x_i = y_i + 1$ then $x_i \geq 1$.
Substituting $y_i = x_i - 1$ into the equations, we get $(y_1 - 1) + (y_2 - 2) + \cdots + (y_r - 1) = n$,
equivalent to

$$y_1 + y_2 + \cdots + y_r = n + r.$$

4.16 Example integer solutions

Note. Counting solutions is not the same as counting portions of n.

Example. How many different solutions are there to: $x_1 + x_2 + x_3 = 11$ so that $x_i \in \mathbb{Z}$ and

(i) $x_i \geq 0, n = 11, r = 3$
$A)$ $\binom{11+3-1}{3-1} = \binom{13}{2}$.
(ii) $x_i \geq -5$. Substitute $x_r = y_i - 5$
$A)$ $y_1 + y_2 + y_3 = 26, y_i \geq 0$.

$$\binom{28}{2}.$$

(iii) $0 \leq x_i \leq 5$ substitute $x_i = -y_i + 5$
$y_1 + y_2 + y_3 = 4, 0 \leq y_i \leq 5$.

$$\binom{6}{2}.\text{(ignore 5)}$$

(iv) $0 \leq x_i \leq 7$ substitute $x_i = -y_i + 7$
$y_1 + y_2 + y_3 = 10, 0 \leq y_i \leq 7$. Here, theorem doesn't apply.