MATH1061 Notes Sem 2 2019

Tom Stephen

October 31, 2019

Contents

1 Logic

1.1 Logical Form

Def. A statement or proposition is a sentence that is either true or false, but not both.

Ex. Statements:

- The number 5 is even
- $\pi > 3$
- Leonhard Euler was born in 1707

Not statements:

- How are you?
- Stop!
- She likes maths. (we do not know who she is)
- $x^2 = 2x - 1$ (we do not know the value of x)

Def. Let p be a statement. The negation of p is denoted as $\sim p$ or $\neg p$ (read as "not p").

p	$\sim p$
T	F
F	T

Let p and q be statements.

Def. The conjunction of p and q is denoted $p \wedge q$ (read as "p and q")

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Def. The disjuction of p and q is denoted $p \vee q$ (read as "p or q")

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Think of p,q,r as statement variables.

Def. A statement form is made up from statement variables (p, q, r) and the symbols $\sim, \wedge, \vee$ with unambiguos parentheses.

Ex.

$$P = \sim (p \vee r) \wedge (\sim r)$$

is a statement form. How many rows will a truth table for P need? We realise we have 3 statement variables, so we will need $2^3 = 8$ rows.

1.2 Logical Equivalence

Def. Two statement forms P and Q are logically equivalent, denoted $P \equiv Q$, if they have identical truth values for every possible combination of truth values for their statement variables.

Ex.

$$\sim (\sim p) \equiv p$$

1.2.1 Demorgan's Law

$$\sim (p \wedge q) \equiv \sim p \vee \sim q$$

$$\sim (p \vee q) \equiv \sim p \wedge \sim q$$

1.2.2 Commutativity

$$p \wedge q \equiv q \wedge p$$

$$p \vee q \equiv q \vee p$$

1.2.3 Associativity

$$p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$$

$$p \vee (q \vee r) \equiv (p \vee q) \vee r$$

1.2.4 Distributive Laws

$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$$

$$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$$

1.2.5 Double Negative

$$\sim (\sim p) \equiv p$$

1.2.6 Idempotent Laws

$$p \wedge p \equiv p$$

$$p \vee p \equiv p$$

1.2.7 Absorption Laws

$$p \vee (p \wedge q) \equiv p$$

$$p \wedge (p \vee q) \equiv p$$

1.2.8 Tautolgy and Contradiction

Def. A tautolgy is a statement form which always takes the truth value *true* for all possible truth values of its variables.

Ex.

p	$\sim p$	$p \vee \sim p$
T	F	T
F	T	T

Def. A contradiction is a statement form which always takes the truth value *false* for all possible truth values of its variables.

Ex.

p	$\sim p$	$p\wedge\sim p$
T	F	F
F	T	F

1.2.9 Identity Laws

$$p \wedge (\text{tautolgy}) \equiv p$$
$$p \vee (\text{contradiction}) \equiv p$$

1.2.10 Universal Bound Law

$$p \vee (\text{tautolgy}) \equiv (\text{tautolgy})$$
$$p \wedge (\text{contradiction}) \equiv (\text{contradiction})$$

1.2.11 Negation Laws

$$p\vee \sim p \equiv \text{tautolgy}$$
$$p\wedge \sim p \equiv \text{contradiction}$$

1.2.12 Negations

$$\sim (\text{tautolgy}) \equiv \text{contradiction}$$
$$\sim (\text{contradiction}) \equiv \text{tautolgy}$$

1.3 Conditional Statements

Def. Let p and q be statement variables. The conditional from p to q, denoted $p \to q$ (read as "p implies q" or "if p then q"), is defined by the following truth table:

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

1.3.1 Expressing the Conditional with Logical Connectives

$$p \to q \equiv \sim p \vee q$$

1.3.2 Contrapositive

Def. The contrapositive of $p \to q$ is $\sim q \to \sim p$. These are logically equivalent.

1.3.3 Negation of $p \to q$

$$\sim (p \to q) \equiv p\wedge \sim q$$

1.3.4 Biconditional Statements

Def. Let p and q be statement variables. The biconditional of p and q, denoted $p \leftrightarrow q$ (read as "p if and only if q"), is defined by the following truth table:

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

1.4 Arguments

Def. Given a collection of statements $p_1, p_2, \dots, p_n$ (called premises) and another statement q (called the conclusion), an argument is the assertion that the conjuction of the premises implies the conclusion. Symbollically, this is represented as

$$\begin{array}{l} p_1 \\ p_2 \\ \vdots \\ p_3 \\ \therefore q \end{array}$$

Def. An argument is valid if whenever all of the premises are true, the conclusion is also true. Thus, an argument is valid if

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \to q$$

is a tautolgy.

1.4.1 Rules of Inference

Modus Ponens

$$\begin{array}{l} p \to q \\ p \\ \therefore q \end{array}$$

Modus Tollens

$$\begin{array}{l} p \to q \\ \sim q \\ \therefore \sim p \end{array}$$

Generalisation

$$\begin{array}{ll} p & q \\ \therefore p \vee q & \therefore p \vee q \end{array}$$

Specialisation

$$\begin{array}{ll} p \wedge q & p \wedge q \\ \therefore p & \therefore q \end{array}$$

Conjuction

$$\begin{array}{l} p \\ q \\ \therefore p \wedge q \end{array}$$

Elimination

$$\begin{array}{ll} p \vee q & p \vee q \\ \sim q & \sim p \\ \therefore p & \therefore q \end{array}$$

Transitivity

$$p \to q$$
$$q \to r$$
$$\therefore p \to r$$

Proof by Division into Cases

$$p \vee q$$
$$p \to r$$
$$q \to r$$
$$\therefore r$$

Contradiction rule

$$\sim p \to \text{(contradiction)}$$
$$\therefore p$$

1.5 Quantified Statements

Def. A predicate is a sentence that contains finitely many variables, and which becomes a statement if the variables are given specific values. The domain of each variable in a predicate is the set of all possible values that may be assigned to it.

Def. The truth set of a predicate $P(x)$ is the set of all values in the domain that, when assigned to x, make $P(x)$ a true statement.

Ex. Let $P(x)$ be the predicate "x divides 5" with the set of integers as the domain of x. The truth set of $P(x)$ is $\{-5, -1, 1, 5\}$

1.5.1 Common Domains

Domain	Symbol	Example
Integers	$\mathbb{Z}$	$\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$
Positive Integers	$\mathbb{Z}^{+}$	$\{1, 2, 3, \dots\}$
Non-negative Integers	$\mathbb{Z}^{\text{nonneg}}$ or $\mathbb{Z}^{\geq 0}$	$\{0, 1, 2, 3, \dots\}$
Natural Numbers	$\mathbb{N}$	$\{1, 2, 3, \dots\}$
Rational Numbers	$\mathbb{Q}$	$\{\frac{a}{b} \mid a, b \in \mathbb{Z} \wedge b \neq 0\}$
Real Numbers	$\mathbb{R}$	the entire number line

Def. The Universal Quanitifier: The symbol $\forall$ denotes "for all" (or "for each" or "for every") and is called the universal quantifier. Let $Q(x)$ be a predicate and D be the domain of x. The universal statement

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

is true if and only if $Q(x)$ is true for every x in D. It is false if and only if $Q(x)$ is false for at least one x in D.

Def. The Existential Quantifier: The symbol $\exists$ denotes "there exists" (or "there is" or "there are") and is called the existential quantifier. Let $Q(x)$ be a predicate and D be the domain of x. The existential statement

$$\exists x \in D \text{ such that } Q(x)$$

is true if and only if $Q(x)$ is true for at least one x in D. It is false if $Q(x)$ is false for every x in D.

1.5.2 Universal Conditional Statements

One of the most important statement forms in mathematics is

$$\forall x \in D \text{ if } P(x) \text{ then } Q(x)$$

or equivalently,

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

1.5.3 Negation

Recall universal statement

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

The negation of this statement is logically equivalent to

$$\exists x \in D \text{ such that } \sim Q(x)$$

Recall existential statement

$$\exists x \in D \text{ such that } R(x)$$

The negation of this statement is logically equivalent to

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

Recall universal conditional statement

$$\forall x \in D \text{ if } P(x) \text{ then } Q(x)$$

The negation of this statement is logically equivalent to

$$\exists x \in D \text{ such that } \sim (P(x) \to Q(x))$$

which is

$$\exists x \in D \text{ such that } P(x) \wedge \sim Q(x)$$

2 Number Theory

2.1 Modulo Arithmetic

2.1.1 Floor and Ceiling

Def. Given any $x \in \mathbb{R}$, the floor of x, denoted $\lfloor x \rfloor$, is the unique integer n such that $n \leq x < n+1$
Given any $x \in \mathbb{R}$, the ceiling of x, denoted $\lceil x \rceil$, is the unique integer n such that $n-1 < x \leq n$

2.2 Euclidean Algorithm

Def. For integers $a, b \in \mathbb{Z}$, not both zero, the greatest common divisor of a and b, denoted $\gcd(a, b)$, is the integer d which satisfies the following two properties:

- $d|a$ and $d|b$
- for all $c \in \mathbb{Z}$, if $c|a$ and $c|b$, then $c \geq d$

Thus d is the largest integer for which $d|a$ and $d|b$

If $\gcd(a, b) = 1$ then a and b have no common factors other than ± 1 and we call a and b coprime or relatively prime.
Fact: If a and b are integers with $b \neq 0$ and if q and r are integers such that

$$a = bq + r$$

then

$$\gcd(a, b) = \gcd(b, r)$$

Def. The Euclidean Algorithm: to find $\gcd(a, b)$ where $a, b \in \mathbb{Z}$ and $a \geq b > 0$,

- write $a = bq + r$, as in the quotient-remainder theorm
- if $r = 0$, then terminate with $\gcd(a, b) = b$
- otherwise replace (a, b) with (b, r) and repeat

Def. For nonzero integers $a, b \in \mathbb{Z}$, the lowest common multiple of a and b is the smallest positive integer n for which $a|n$ and $b|n$. We write this as $\operatorname{lcm}(a, b)$

Fact: suppose $a, b \in \mathbb{Z}$ where $a \geq b > 0$. Then

$$\gcd(a, b) \cdot \operatorname{lcm}(a, b) = a \cdot b$$

2.3 Sequences

Def. A sequence is an ordered list of elements. It can be infinite or finite. Each individual element is called a term. We often denote the terms of sequences by lower case letters with subscripts.

An explicit formula or general formula for a sequence is a rule showing how the value of a general term a_k depends upon k.

Ex.

$$1, 2, 3, 4, 5, \ldots$$

The listed terms $a_0, a_1, a_2, \ldots$ follow a pattern, where $a_k = 2^k$.
Different notations are used to denote such a sequence, such as

$$\left\{2^k\right\}_{k\geq 0} \text{ or } \left\{2^k\right\}_{k=0}^{\infty} \text{ or } \left(2^k\right)_{k\geq 0} \text{ or } \left(2^k\right)_{k=0}^{\infty}$$

Ex. Write the first 5 terms of $\left\{\frac{(-1)^n}{n}\right\}_{n\geq 1}$

$$a_1 = -1,\ a_2 = \frac{1}{2},\ a_3 = -\frac{1}{3},\ a_4 = \frac{1}{4},\ a_5 = -\frac{1}{5}$$

Def. An alternating sequence is a sequence in which the terms alternate between postive and negative, such as the previous example.

It is often useful to find a general term from initial terms.

Ex. Find a general formula for a sequence that has the following initial terms

$$2, \frac{3}{4}, \frac{4}{9}, \frac{5}{16}, \frac{6}{25}, \frac{7}{36}, \ldots$$

Let a_n denote the general term and suppose the initial term is a_1. Observe that the denominator of each term is a perfect square and we can rewrite the terms as

$$\frac{1+1}{1^2}, \frac{2+1}{2^2}, \frac{3+1}{3^2}, \frac{4+1}{4^2}, \frac{5+1}{5^2}, \frac{6+1}{6^2}, \ldots$$

Thus, the general term

$$a_n = \frac{n+1}{n^2}$$

or, the sequence $\left\{\frac{n+1}{n^2}\right\}_{n\geq 1}$ has the given initial terms.

2.4 Summation Notation

We use greek capital Sigma Σ to indicate a sum. If $m, n \in \mathbb{Z}$ and $m \leq n$, then

$$\sum_{i=m}^{n} a_i = a_m + a_{m+1} + \cdots + a_{n-1} + a_n$$

2.5 Dummy Variable

Ex. The variable i is $\sum a_i$ is a dummy variable. You can use any letter here, as long as it does not have another meaning.

2.6 Product Notation

We use greek capital Pi Π to indicate a product. If $m, n \in \mathbb{Z}$ and $m \leq n$, then

$$\prod_{i=m}^{n} a_i = a_m \cdot a_{m+1} \cdot \dots \cdot a_{n-1} \cdot a_n$$

2.7 Factorial

For $n \in \mathbb{Z}^+$, we define $n!$ (read "n factorial") to be

$$n! = n(n-1)(n-2) \cdot \dots \cdot 3 \cdot 2 \cdot 1 = \prod_{i=1}^{n}$$

also, $0! = 1$

2.8 Properties of Summation and Product Notation

If a_m, a_{m+1}, a_{m+2}, $\dots$ and b_m, b_{m+1}, b_{m+2}, $\dots$ are sequences of real numbers, and c is any real number, then, for any interger $n \geq m$, the following hold.

1. $\sum_{i=m}^{n} a_i \pm \sum_{i=m}^{n} b_1 = \sum_{i=m}^{n} a_i \pm b_i$
2. $\sum_{i=m}^{n} ca_i = c \sum_{i=m}^{n} a_i$
3. $\left(\prod_{i=m}^{n} a_i\right)\left(\prod_{i=m}^{n} b_1\right) = \prod_{i=m}^{n} a_i b_i$

2.9 Mathematical Induction

Def. The Principle of Mathematical Induction.
Let $P(n)$ be a predicate that is defined for every integer $n \geq a$, where a is some fixed integer. Suppose

1. $P(a)$ is true.
2. For every integer $k \geq a$, $P(k) \rightarrow P(k+1)$

Then $P(n)$ is true for every integer $n \geq a$

2.9.1 Strong Mathematical Induction

Def. The Principle of Strong Mathematical Induction.
Let $P(n)$ be a predicate that is defined for every integer $n \geq a$, where a is some fixed integer, and let b be an integer where $b \geq a$. Suppose:

- *Base step*: $P(a)$, $P(a+1)$, $\dots$, $P(b)$ are all true
- *Inductive Step*: For every integer $x \geq b$, if $P(a)$, $P(a+1)$, $\dots$, $P(k)$ are all true, then $P(k+1)$ is true.

The $P(n)$ is true for every integer $n \geq a$.

Prove that for every integer $n \geq 8$, we can form n cent postage using only 3c and/or 5c stamps.

Before starting a proof, we observe:

$$\begin{aligned}
8 &= 5+3 \to 11 = (5+3)+3 \\
9 &= 3+3+3 \to 12 = (3+3+3)+3 \\
10 &= 5+5 \to 13 = (5+5)+3
\end{aligned}$$

We can now use this idea in a formal proof.

Proof. Let $P(n)$ be the predicate "n cent postage can be formed using only 3c and/or 5c stamps"
Basis Step: We can prove $P(8)$, $P(9)$, $P(10)$ direction, since

$$\begin{aligned}
8 &= 5+3 \\
9 &= 3+3+3 \\
10 &= 5+5
\end{aligned}$$

Inductive Hypothesis: Suppose that for some integer $k \geq 10$, $P(8), \ldots, P(k)$ are all true. We will use this to prove $P(k+1)$.
Since $k \geq 10$, we have $k-2 \geq 8$. Thus, by the Inductive Hypothesis, we can form $(k-2)c$ using 3c and 5c stamps. Now we can add 1 more 3c stamp to make $(k+1)c$ postage and so $P(k+1)$ is true.
Therefore, by strong induction, it follows that $P(n)$ is true for every integer $n \geq 8$. □

2.9.2 Well Ordering Principle

Def. The *Well Ordering Principle* for the integers.
If S is a non-empty set of integers, all of whihc are greater than some fixed integer, then S has a least element.

3 Recursive Defintions

Ex. The sequence

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots$$

is called the Fibonacci Sequence

Def. A recurrence relation for a sequence $a_0, a_1, a_2, \ldots$ is a formula that relates each term a_k to some of its predecessors $a_{k-1}, \ldots, a_{k-i}$ where $i \in \mathbb{Z}$ and $k - i \geq 0$
The initial conditions for such a recurrence relation specify the values of some of the intial terms.

Ex. The Fibonacci sequence is defined recursively by

$$F_0 = 1,\ F_1 = 1, \text{ and } F_n = F_{n-1} + F_{n-2}$$

3.1 Ways to Define Sequences

A sequence can be defined

- *informally*, by listing the first few terms of the sequence until the pattern becomes obvious
- *with a general formuka*, by stating how a term a_n depends on n and stating where it starts
- *recursively*, by giving a recurrence relation relating terms in the sequence to earlier ones and also some intial conditions

3.2 Showing a Sequence Satisfies a Recurrence Relation

Ex. Show that the sequence

$$a_k = 3 \cdot 2^k, \text{ for } k \geq 0$$

satisfies the recurrence relation

$$a_n = 2a_{n-1}, \text{ for } n \geq 1$$

The sequence is $\left\{3 \cdot 2^k\right\}_{k \geq 0} = 3,\ 6,\ 12,\ 24,\ 48,\ dots$
For every integer $n \geq 1$ we have $a_n = 3 \cdot 2^n$ and $a_{n-1} = 3 \cdot 2^{n-1}$
Hence,

$$a_n = 3 \cdot 2^n = 3 \cdot 2 \cdot 2^{n-1} = 2(3 \cdot 2^{n-1}) = 2a_{n-1}$$

3.3 Generalised

We have seen that sequences of numbers can be defined recursively. Many other objects can be defined recursively as well, such as: sets, sums, products and function.
A recursive definition for a set of objects requires three things:

1. BASE: a statement that a certain object belongs in the set
2. RECURSION: a collection of rules showing how to form new objects for the set from existing ones in the set
3. RESTRICTION: a statement that no objects belong to the set other than those arising from steps 1 and 2

Ex. Consider the set of all valid bracketings. Every left bracket (is matched with a right bracket) and at every stage, reading left to right, there are at least as many left brackets as right brackets.

(())() is valid

()()() is valid

())(() is invalid

Recursive definition of the set of valid brakcetings

1. Base: an empty expression with no brackets is valid
2. Recursion:
   (a) if B is valid, the (B) is also valid
   (b) if B and C are valid, then BC is also valid
3. Restriction: Any expression not derived from the rules above is not valid

3.4 Solving Recurrence Relations

4 Functions

4.1 One-to-one

Def. Let f be a funciton from a set X to a set Y. The function f is one-to-one (or injective) if and only if for all elements x_1 and x_2 in X,

$$\text{if } f(x_1) = f(x_2), \text{ then } x_1 = x_2$$

Or, equivalently, for all elements x_1 and x_2 in X,

$$\text{if } x_1 \neq x_2, \text{ then } f(x_1) \neq f(x_2)$$

A function $f : X \to Y$ is not one-to-one if and only if there exist some x_1 and x_2 in X such that $f(x_1) = f(x_2)$ and $x_1 \neq x_2$

1. To prove a function $f : X \to Y$ is one-to-one, we typically use a direct proof:
   (a) suppose x_1 and x_2 are element of X, and $f(x_1) = f(x_2)$
   (b) show that $x_1 = x_2$
2. To prove that a function $f : X \to Y$ is not one-to-one, we typically find elements x_1 and x_2 in X such that $f(x_1) = f(x_2)$ but $x_1 \neq x_2$

Ex. Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2$. Is f one-to-one?
Proof that f is not one-to-one:

Proof. Take $x_1 = 2$ and $x_2 = -2$
Since $f(2) = 4$ and $f(-2) = 4$, we have found different elements of the domain with the same image. Thus f is not one-to-one. □

4.2 Onto

Def. Let f be a function from a set X to a set Y. The function f is onto (or subjective) if and only if given any element $y \in Y$, it is possible to find an element $x \in X$ with the property that $y = f(x)$.
Equivalently, $f : X \to Y$ is onto if and only if $\forall y \in Y$, $\exists x \in X$ such that $f(x) = y$
A function $f : X \to Y$ is not onto if and only if there exists some $y \in Y$ such that for all $x \in X$, $f(x) \neq y$.

- To prove that a function $f : X \to Y$ is onto, we usually
  - suppose that $y \in Y$
  - construct an element x of X with $f(x) = y$
- To prove that a function $f : X \to Y$ is not onto, we usually
  - find an element $y \in Y$ such that $y \neq f(x)$ for any $x \in X$

4.3 Inverse

5 Set Theory

Together with logic, set theory provides a significant foundation of mathematics.

Def. A set S is a collection of objects, which are called the elements of S.
If x is in S, we write $x \in S$. If not, we write $x \notin S$.
We can sometimes list the elements of S with curly braces:

$$S = \{x_1, x_2, x_3, \dots\}$$

The order of elements, and repetitions are ignored.

You may define a set by a *property* that its element must satisfy.

$$A = \{x \in S | P(x)\}$$

means that the elements of A are precisely those elements of S for which he predicate $P(x)$ is true.
The elements of a set can be sets themselves.

Def. If A and B are sets, A is called a subset of B, written $A \subseteq B$, if and only if every element of A is also an element of B.

$$A \subseteq B \implies \forall x, x \in A \to x \in B$$

Note: every set is a subset of itself.

Def. Two sets are equal if they contain the same elements.

Def. The empty set is the set containing no elements and is denoted by $\emptyset$.

$$\emptyset = \{\}$$

5.1 Operations on Sets

Let A and B be any sets.
The union of sets A and B, denoted $A \cup B$, is the set of all elements x such that $x \in A$ or $x \in B$ (or both).

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

The intersection of sets A and B, denoted $A \cap B$, is the set of all elements x such that $x \in A$ and $x \in B$.

$$A \cap B = \{x | x \in A \text{ and } x \in B\}$$

The set difference of B minus A, denoted $B - A$, and sometimes $B \setminus A$, is the set of all elements x such that $x \in B$ and $x \notin A$.

$$B - A = \{x | x \in B \text{ and } x \notin A\}$$

If the sets we are considering are all subsets of some set U, called the universal set, then $U - A$ is called the complement of A and is denoted A^c.

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

5.2 More Definitions for Sets

Def. For any set S, the power set of S, denoted by $\mathcal{P}(S)$, is the set of all subsets of S.

$$\mathcal{P}(S) = \{X | X \subseteq S\}$$

Ex. For set $S = \{1, 3\}$, the power set will be $\mathcal{P}(S) = \{\emptyset, \{1\}, \{3\}, \{1, 3\}\}$

If $|S| = n$, then $|\mathcal{P}(S)| = 2^n$

Def. Two sets A and B are disjoint if and only if $A \cap B = \emptyset$

Def. Sets $A_1, A_2, A_3, \ldots$ are mutually disjoint (or pairwise disjoint or nonoverlapping) if and only if $A_i \cap A_j = \emptyset$ whenever $i \neq j$.

Def. A finite or infinite collection of nonempty sets $\{A_1, A_2, A_3 \ldots\}$ is a partition of a set A if and only if A is the union of all the A_i and $A_1, A_2, A_3, \ldots$ are mutually disjoint.

Def. Let $n \in \mathbb{Z}^+$ and let $x_1, x_2, \ldots, x_n$ be n not necessarily distinct elements. The ordered n-tuple, denoted $(x_1, x_2, \ldots, x_n)$, consists of the n elements with their ordering: first x_1, then x_2, and so on up to x_n.
When $n = 2$, we call this an ordered pair. When $n = 3$, we call this can ordered triple.

Def. The Cartesian Product of sets A and B, denoted $A \times B$ is

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

5.3 Intervals

Given $a, b \in \mathbb{R}$ with $a \leq b$,

$$(a, b) = \{x \in \mathbb{R} | a < x < b\} \quad \text{open interval}$$

$$[a, b] = \{x \in \mathbb{R} | a \leq x \leq b\} \quad \text{closed interval}$$

$$(a, b] = \{x \in \mathbb{R} | a < x \leq b\} \quad \text{closed interval}$$

and similarly for $[a, b)$.

5.4 Cardinality

Def. The cardinality of a set is a measure of how large it is.
We say that two sets X and Y have the same cardinality if and only if there is a bijection between them.
We write this as $|X| = |Y|$

If $|X| = |Y|$ and $|Y| = |Z|$, then $|X| = |Z|$

A <u>finite</u> set is either one which has no elements at all, or one for which there exists a bijection with a set of the form $\{1, 2, \ldots, n\}$ for some fixed positive integer n.
An <u>infinite</u> set is a non-empty set for which there does not exist any bijection with aa set of the form $\{1, 2 \ldots, n\}$ for any positive integer n.

5.4.1 Finite Sets

Theorm. Suppose X and Y are finite sets.

1. if $|X| > |Y|$, then there is no injective function $f : X \to Y$
2. if $|X| < |Y|$, then there is no surjective function $f : X \to Y$
3. There is a bijection $f : X \to Y$ if and only if $|X| = |Y|$

<u>Corollary</u>: For finite sets X and Y with $|X| = |Y|$, the following statements are equivalent:

$$f : X \to Y \qquad \text{is injective}$$

$$f : X \to Y \qquad \text{is surjective}$$

$$f : X \to Y \qquad \text{is bijective}$$

5.4.2 Infinite Sets

Let $2\mathbb{Z} = \{n | n = 2k \text{ for some } k \in \mathbb{Z}\}$. Prove that $|\mathbb{Z}| = |2\mathbb{Z}|$

Proof. Define a function $f : \mathbb{Z} \to 2\mathbb{Z}$ as follows:

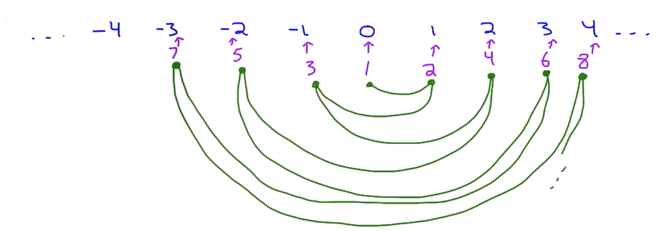
$$f(k) = 2k \qquad \text{for every } k \in \mathbb{Z}$$

<u>To show f is injective</u>: Suppose $k_1, k_2 \in \mathbb{Z}$ and $f(k_1) = f(k_2)$. Then $2k_1 = 2k_2$, so, by dividing both sides by 2, we have $k_1 = k_2$. Hence f is injective.
<u>To show f is surjective</u>: Suppose $n \in 2\mathbb{Z}$. Then $n = 2k$ for some $k \in \mathbb{Z}$. Hence $f(k) = 2k = n$ so f is surjective.
Thus f is a bijection from $\mathbb{Z}$ to $2\mathbb{Z}$

$$\therefore |\mathbb{Z}| = |2\mathbb{Z}|$$

□

Fact: $|\mathbb{Z}^+| = |\mathbb{Z}|$.



The function $f : \mathbb{Z}^+ \to \mathbb{Z}$ defined by

$$f(n) = \frac{n}{2} \qquad \text{if } n \in \mathbb{Z}^+ \text{ is even}$$

$$f(n) = -\frac{n-1}{2} \qquad \text{if } n \in \mathbb{Z}^+ \text{ is odd}$$

is a bijection.

5.5 Counting Sets

Def. A set is called countably infinite if and only if it has the same cardinality as the set of postive integers $\mathbb{Z}^+$

Ex. $\mathbb{Z}$, $2\mathbb{Z}$, $\mathbb{Q}^+$, $\mathbb{Q}$ are all countably infinite.

Def. A set is called countable if and only if it is infinite or countably infinite. A set that is not countable is called uncountable.

Theorm. Any subset of any countable set is countable.

Corollary: any set with an uncountable subset is uncountable.

Theorm. The set $\{x \in \mathbb{R} | 0 < x < 1\}$ is uncountable.

Note: every real number between 0 and 1 has a unique decimal representation except that

$$0.199999\cdots = 0.2000\ldots$$

and for such numbers, we agree to take the one that ends in all 0's.

Proof. Suppose the theorm is false. Then $\{x \in \mathbb{R} | 0 < x < 1\}$ is countable, so the decimal representations of these numbers can be written in a list.

$$\begin{gathered} 0.a_{11}a_{12}a_{13}a_{14}\ldots a_{1n}\ldots \\ 0.a_{21}a_{22}a_{23}a_{24}\ldots a_{2n}\ldots \\ 0.a_{31}a_{32}a_{33}a_{34}\ldots a_{3n}\ldots \\ \vdots \end{gathered}$$

We now construct a new decimal number

$$d = 0.d_1d_2d_3\ldots d_n\ldots$$

as follows

$$\begin{cases} 1 & \text{if } a_{nn} \neq 1 \\ 2 & \text{if } a_{nn} = 1 \end{cases}$$

For instance, take the above a numbers as

$$\begin{gathered} 0.120411\ldots \\ 0.201377\ldots \\ 0.135600\ldots \\ 0.897124\ldots \\ \vdots \end{gathered}$$

So

$$d = 0.2112\ldots$$

Note that for each integer $n \in \mathbb{Z}^+$, d differs from the n^{th} real number in the list because it differs in the n^{th} decimal place.
Thus, $d \in \{x \in \mathbb{R} | 0 < x < 1\}$ but d does not belong to the list of all real numbers between 0 and 1, which is a contradiction.
Therefore $\{x \in \mathbb{R} | 0 < x < 1\}$ is uncountable. $\square$

This shows that since $(0, 1) \subseteq \mathbb{R}$ and $(0, 1)$ is uncountable, $\mathbb{R}$ is uncountable.

5.5.1 Comparing Cardinalities

1. $|X| \leq |Y|$ if and only if $\exists$ injective $f : X \to Y$
2. $|X| \geq |Y|$ if and only if $\exists$ surjective $f : X \to Y$
3. $|X| < |Y|$ if and only if
   (a) $\exists f : X \to Y$ such that f is injective
   (b) $\nexists f : X \to Y$ such that f is bijective
4. $|X| > |Y|$ if and only if
   (a) $\exists f : X \to Y$ such that f is surjective
   (b) $\nexists f : X \to Y$ such that f is bijective

Def. $|0| < |X|$ and $|X| > |0|$ for all $X \neq 0$

5.5.2 The Schroder-Bernstein Theorm

If $|X| \leq |Y|$ and $|X| \geq |Y|$, then $|X| = |Y|$.
Thus, to show $|X| = |Y|$, it is enough to find

1. an injective function $X \to Y$ and
2. a surjective function $X \to Y$

OR

1. an injective function $X \to Y$ and
2. an injective function $Y \to X$

OR

1. a surjective function $X \to Y$ and
2. a surjective function $Y \to X$

This can be much easier than finding a bijection.

Ex. Show $|\mathbb{Z}^+| = |\mathbb{Q}^+|$ using the Schroder-Bernstein theorm.

1. The function $f : \mathbb{Z}^+ \to Q^+$ is defined by $f(n) = n \, \forall n \in \mathbb{Z}^+$ is injective $\therefore |\mathbb{Z}^+| \leq |\mathbb{Q}^+|$
2. Let $g : \mathbb{Q}^+ \to \mathbb{Z}^+$ be defined as follows: for each $q \in \mathbb{Q}^+$, let $q = \frac{a}{b}$ where $a, b \in \mathbb{Z}^+$, $b \neq 0$ and $\gcd(a, b) = 1$ and let $g(q) = 2^a 3^b$.

Proof that g is injective:
Let $q_1 = \frac{a}{b}$ and $q_2 = \frac{c}{d}$ as described above and suppose $g(q_1) = g(q_2)$. Then $2^a 3^b = 2^c 3^d$. By unique prime factorisation, $a = c$ and $b = d$. Hence, $q_1 = q_2$ so g is injective. $\therefore |\mathbb{Q}^+| \leq |\mathbb{Z}^+|$.

5.6 Relations on Sets

Def. Given sets A and B, a <u>binary relation</u> R from A to B is a subset of $A \times B$. If $(x, y) \in \mathbb{R}$ we also write xRy and say that x is <u>related</u> to y. Other symbols may be used to denote a relation $(\rho, \sigma, \tau$, etc)

Def. If R is a binary relation from A to B, the the inverse relation R^{-1} is defined from B to A by

$$R^{-1} = \{(b,a) \in B \times A | (a,b) \in R\}$$

So for all $a \in A$ and $b \in B$,

$$(b,a) \in R^{-1} \text{ if and only if } (a,b) \in R$$

6 Groups

Def. Let G be a set and let $*$ be a binary operation $* : G \to G$. We call $(G, *)$ a *group* if it has the following properties:

1. Closure: for all $g,\ h \in G,\ g * h \in G$
2. Associative: for all $g, h, k \in G,\ (g * h) * k = g * (h * k)$
3. Identity: there exists some element $e \in G$ such that $e * g = g * e = g\ \forall g \in G$
4. Inverses: for all $g \in G$ there exists some element $g^{-1} \in G$ such that $g * g^{-1} = g^{-1}g = e$

Def. For a positive integer n, let $\mathbb{Z}_n$ denote the equivalence classes of integers modulo n

$$\mathbb{Z}_n = \{[0],\ [1],\ [2],\ \ldots,\ [n-1]\}$$

Define $+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ by

$$[a] + [b] = [a + b]$$

Define $\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ by

$$[a] \cdot [b] = [a \cdot b]$$

6.1 Subgroup

Def. Let $(G, *)$ be a group and let $H \subseteq G$. We say that H is a *subgroup* of G if $(H, *)$ is itself a group. That is, it is a subgroup of G if

1. for all $g, h \in H$, we have $g * h \in H$ (closure)
2. if e is the indentity for $(G, *)$ then $e \in H$ (identity)
3. for all $h \in H$, if h^{-1} is the inverse of h in $(G, *)$, then $h^{-1} \in H$ (inverses)

We write $H \leq G$ to denote H is a subgroup of G, when the context of groups is clear (i.e. not leq).
If $H \leq G$ and $H \neq G$, we say H is a <u>proper</u> subgroup of G.
If e is the indentity of group G, the <u>trivial</u> subgroup of G is $\{e\}$.

7 Counting

Ex. Suppose a restaurant has 5 types of cake and 2 types of icecream to select for dessert.

1. How many choices for dessert are there if you select one cake and one icecream? There are $5 \cdot 2 = 10$ choices. *This is a sequence of tasks - first, choose a dessert, then, choose an icecream.*

2. How many choices for dessert are there if you select either one cake or one icecream, but not both? There are $5 + 2 = 7$ choices. *These are two distinct cases.*

Ex. Consider a password consisting of 3 letters from the set $\{A, B, C, \ldots, Z\}$.

1. How many passwords are possible? There are 26 choices for each of the 1st, 2nd and 3rd letters, so there are
$$26 \cdot 26 \cdot 26 = 17576 \text{ possiblities}$$

2. How many passwords contain no repeated letters? There are 26 letters for the 1st letter, 25 for the 2nd and 24 for the 3rd.
$$\therefore 26 \cdot 25 \cdot 24 = 15600 \text{ possiblities}$$

3. How many passwords use only vowels or only consonants?
$$\text{option 1 (only vowels) } + \text{option 2 (only consonants)}$$
$$5^3 + 21^3 = 9386$$

Def. A <u>permutation</u> of a set of objects is an arrangement of the objects into an order.

Ex. How many permutations of the letters in the word *SWITCH* are there? i.e. SWITCH, CWITHS, etc.

$$\# \text{ of these} = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 6! = 720$$

Theorm. For any $n \in \mathbb{Z}^+$, the number of permutations of a set with n elements is $n!$.

Ex. Consider the permutations of the letters of the word *OBJECTS*. How many permutations start with a vowel?
Option 1: start with "o": $6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 6!$
Option 2: start with "e": $6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 6!$
Answer: $6! + 6! = 1440$.

Ex. Consider all license plates consisting of 3 digits from the set $\{0, 1, \ldots, 9\}$ followed by 3 letters from the set $\{A, B, \ldots, Z\}$

1. How many license plates are possible?

$$10 \cdot 10 \cdot 10 \cdot 26 \cdot 26 \cdot 26 = 17576000$$

2. How many license plates have no repeated symbols?

$$10 \cdot 9 \cdot 8 \cdot 26 \cdot 25 \cdot 24 = 11232000$$

3. How many license plates have at least one repeated symbol? We know the total number of license plates and the number of those with no repeated symbols, so the rest must have at least one repeated symbol.

$$\therefore 17576000 - 11232000 = 6344000$$

Let n and r to be nonnegative integers.
Problem: *Select r elements from a set containing n elements. How many ways are there to do the selection?*
The answer depends on:

- whether or not order matters
- whether or not repetition is allowed

Case where order matters and repetition is allowed.

Ex. We have a new ATM card and need to select a PIN. We may choose four digits from the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Order matters, and we may repeat. How many PINs are there?
In each of the four selections we have 10 choices, and hence there are 10^4 possiblities.

Fact: the number of selections of r elements from a set containing n elements where order matters and repetition is allowed is n^r.
Case where order matters, and there is no repetition.

Ex. If there are 7 runners, how many ways can 1st, 2nd and 3rd be awarded?

$$7 \cdot 6 \cdot 5 = 210$$

Def. Let n and r be nonnegative integers with $r \leq n$. An r-permutation of a set of n elements is an ordered selection of r elements taken from the set of n elements. The number of r-permutations of a set of n elements is denoted $P(n, r)$ or nPr.

Theorm. If $n, r \in \mathbb{Z}$ and $1 \leq r \leq n$, then

$$P(n, r) = n(n-1)(n-2)\ldots(n-r+1) = \frac{n!}{(n-r)!}$$

Case where order doesn't matter, and repetition is not allowed.

Ex. In how many ways can 5 students be selected from a class of 15 to form a committee?
If we assume order did matter, we would count as in case 2, to get

$$15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 = 360360$$

But order does not matter, and each set of students was counted $5! = 120$ times, so the actual number of choices is

$$\frac{360360}{120} = 3003$$

Def. Let n and r be nonnegative integers with $r \leq n$. An r-combination of a set of n elements is a subset of r of the n elements. The number of r-combinations of a set of n elements is denotes $C(n, r)$ or nCr or, more commonly, $\binom{n}{r}$ which is read "n choose r".

Theorm. If n and r are nonnegative integers and $r \leq n$, then

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

Case where order does not matter, and repetition is allowed.

Ex. Suppose a store has 4 large buckets, each with a different type of coloured candy: red, blue, yellow, pink. If you must select a total of 7 candies, how many different choices do you have?
Select 7 elements from $\{r, b, y, p\}$ (repetition allowed) where order doesn't matter (i.e. "rrbbyyy" is the same as "ryrybby")
Answer = 120.

Ex. How many permutations of the letters "ALFALFA" are there?
Method (1).

- select positions for the 3 A's
- select positions for the 2 F's
- put the 2 L's in the remaining positions

Answer:

$$\binom{7}{3} \cdot \binom{4}{2} \cdot 1 = 35 \cdot 6 = 210$$

note the 1 is really $\binom{2}{2} = 1$
Method (2). if the letters were distinct,

$$A_1 A_2 A_3 F_1 F_2 L_1 L_2$$

there would be $7! = 5040$ possiblities. Now, make the 3 A's indistinguishable. We have counted

$$A_1 F_1 F_2 L_2 L_1 A_2 A_3$$

and

$$A_2 F_1 F_2 L_2 L_1 A_1 A_3$$

as different solutions, so we have overcounted by $3! = 6$ times. Thus, $\frac{5040}{6} = 840$ possible solutions.
Now make the 2 F's indistinguishable: we have overcounted by 2 times, so we have $\frac{840}{2!} = 420$ possible solutions. Finally, make the 2 L's indistinguishable: we have overcounted by 2! times, so we have $\frac{420}{2!} = 210$ possible solutions.

Theorm. Suppose you have n objects of which n_1 are if type 1, n_2 are of type 2, etc. The number of distinct permutations of the n objects is

$$\binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n)3}\dots\binom{n-n_1-n_2-\dots-n_{k-1}}{n_k} = \frac{n!}{n_1!n_2!\dots n_k!}$$

7.1 Inclusion and Exclusion

Ex. In a fishtank, there are 14 blue fish, 7 striped fish, and 4 fish that are both blue and striped. How many fish are blue or striped?
If we add the blue fish and the striped fish, we get $14 + 7 = 21$. However, we counted the blue striped fish twice (once for being blue, once for being striped), so the actual answer is $(14 + 7) - 4 = 17$.

Theorm. Let A and B be disjoint finite sets, the $|A \cup B| = |A| + |B|$

More generally,

Theorm. For any finite sets A and B, $|A \cup B| = |A| + |B| - |A \cap B|$

Def. The Inclusion/Exclusion Principle (for 2 or 3 sets)...
If A, B, C are any finite sets, then

$$|A \cup B| = |A| + |B| - |A \cap B|$$

and

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

7.2 Pigeonhole Principle

Def. The Pigeonhole Principle: Suppose you have n pigeons sitting in k pigeonholes. If $n > k$, then at least one of the pigeonholes contains at least two pigeons.

Ex. 5 pigeons, 4 holes, at least 1 hole must have more than 1 pigeon.

Equivalently, a function from a finite set to a smaller finite set cannot be one-to-one.

The contrapositive of the pigeonhole principle is: Suppose you have n pigeons sitting in k pigeonholes. If each pigeonhole contains at most one pigeon, then $n \leq k$.

Ex. If you have 3 different colours in your drawer, what is the minimum number of socks you need to pull out in order to guarantee a matching pair?
Think of pigeons = socks, pigeonholes = colours. Pull out 4 socks to guarantee that at least two of them have the same colour.

Ex. There are 680 people in a list. Must there be at least two people on the list with the same first and last initials? Explain.
pigeons = people, pigeonholes = initials.
There are $26 \cdot 26 = 676$ possible options for first and last initials. Since $680 > 676$, the pigeonhole princple implies at least 2 people must have the same intials.

Def. The generalised pigeonhole principle
Suppose you have n pigeons sitting in k pigeonholes. If $n > k \cdot m$, then at least one of the pigeonholes contains at least $m+1$ pigeons.
Contrapositive: suppose you have n pigeons sitting in k pigeonholes. If each pigeonhole contains at most m pigeons, then $n \leq km$.

Ex. Show that in a group of 25 people, at least 3 must be born in the same month.
Let $n = 25$ and $m = 2$.
We have 25 pigeons (people) and 12 pigeonholes (months).
Since $n > 12 \cdot 2$, the generalised pigeonhole principle implies that there is a month which ≥ 3 people from the group have a birthday.

8 Graph Theory

Before we begin with formal definitions, let us start with an example. Suppose we have a group of people and some of them are friends. We may represent these by drawing a point for each person, and a line for each friendship. Obviously, the position of the dots and lines does *not* matter, just the connections.

Def. A *graph* G consists of two finite sets:

- a non-empty set $V(G)$ of vertices, and
- a (possibly empty) set $E(G)$ of edges, where each edge is associated with a set $\{v, w\} \subseteq V(G)$

The vertices v and w are called the end points of the edge.

Ex.

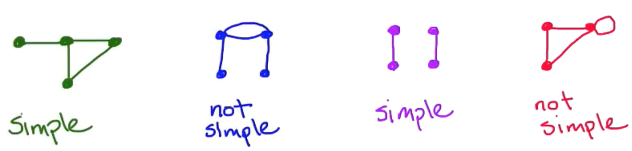
This graph G has $V(G) = \{a,\, b,\, c,\, d\}$ and has 4 edges whose endpoints are

$$\{a,\, b\}\,,\ \{b,\, c\}\,,\ \{c,\, d\}\,,\ \{a,\, d\}$$

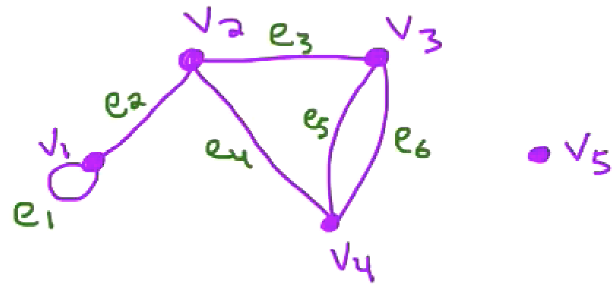
Def. A loop is an edge wose endpoints are equal, which is denoted $\{v,\, v\}$ or $\{v\}$

Def. Parallel edges (or multiple edges) are two or more edges with the same set of endpoints.

Def. A simple graph is a graph with no loops or parallel edges.



Ex. Referred to below.



Def. An edge and a vertex are incident if and only if the vertex is an endpoint of the edge.

Ex. e_3 is incident with v_2 and v_3. v_1 is incident with e_1 and e_2.

Def. Two edges are adjacent if they are incident with the same vertex.
The vertices are adjacent if they are connected by an edge (ie there is an edge they are both incident with).

Ex. e_2 and e_3 are adjacent. v_2 and v_4 are adjacent. v_1 and v_4 are non-adjacent.

Def. An isolated vertex is a vertex which is incident with no edges. Namely, v_5 above.

Def. The degree of a vertex v is the number of edges indcident with v, where we count each loop *twice*. We write this as $\deg(v)$.

Theorm. The Handshake Theorm
Let G be a graph with n vertices

$$V(G) = \{v_1, v_2, v_3, \ldots, v_n\}$$

Then

$$\sum_{i=1}^{n} \deg(v_i) = \deg(v_1) + \deg(v_2) + \cdots + \deg(v_n) = 2 \cdot |E(G)|$$

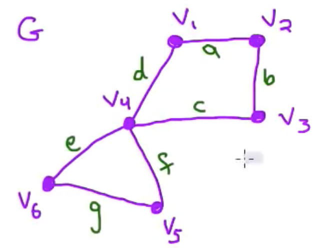
8.1 Getting Between Vertices

Let G be graph and let v and w be vertices in G. A *walk* from v to w is a finite alternating sequence

$$v_0 e_1 v_1 e_2 \ldots v_{n-1} e_n v_n \tag{1}$$

of vertices and edges where $v_0 = v$, $v_n = w$, and e_i is an edge with endpoints $\{v_{i-1}, v_i\}$ for $i \in \{1, \ldots, n\}$

Ex.



$v_5 f v_4 c v_3 c v_4 e v_6$ is a walk from v_5 to v_6.
Also, $v_5 g v_6$ is a walk from v_5 to v_6.

Def. A graph G is connected if and only if, given any two vertices v and w in G, there is a walk from v to w.
A trail is a walk whose edges are distinct.
A circuit is a trail that starts and ends at the same vertex.

Def. Let G be a graph. An Euler circuit for G is a circuit that contains every edge of G exactly once.
Lemma: if a graph G has an Euler circuit, then each vertex has even degree. Proof in lec 35.

Theorm. Let G be a connected graph. Then G has an Euler circuit if and only if every vertex of G has even degree.

Def. Let G be a graph and let u, $v \in V(G)$. An Euler trail from u to v is a trail from u to v that uses every edge exactly once.