MATH1081 DISCRETE MATHEMATICS

P.G. Brown with contributions from D. Angell and D. Tacon.

2016

Chapter 3 - Proofs, Induction and Logic.

1. Proofs

Proof is what distinguishes Mathematics from other disciplines.
Mathematical Proof consists of logical deduction (using agreed logic or argument) from agreed premises.

Scientific Proof is achieved through observation and mathematical models/theory.
When someone claims to have proved something (outside of Mathematics) they really mean that their statement is 'very likely'.

Why do we need proof in mathematics?

Ex. The founder of number theory, Pierre Fermat (died 1665) believed that all integers of the form $2^{2^n}+1$, for $n = 0, 1, 2, 3, ...$ are always prime and this is true for the first 5 values of n, viz., 3,5,17,257,65537, but the next number is 4294967297, which in fact equals 641 times 6700417 and so is not prime. In fact, no known value of n beyond 5 makes $2^{2^n}+1$ prime!

Ex. $n^2 - n + 41$ is prime for all n from 0 to 40, and $n^2 - 79n + 1601$ gives primes for integer values of n from 0 to 79.

One cannot rely on the fact that things seem to be true for a small number of cases, as this is no guarantee that they will be true in all cases. A proof (if one exists) is required.

"Calculator Proof":

In light of what was I said above, we see that calculators cannot be used to give a 'proof' of a mathematical result.

For example, consider the number

$$e^{\pi\sqrt{163}} = 262537412640768743.999999999....$$

Can we conclude that $e^{\pi\sqrt{163}}$ is an integer? No, since the next digit is 2.

On the other hand, my (old) calculator gives

$$\sqrt[3]{2+\sqrt{5}}+\sqrt[3]{2-\sqrt{5}}=0.999996...$$

but in fact the true value is 1.

Computers are subject to alpha particle decay which causes random errors. Contrary to popular belief they are capable of making errors. Can we then rely on them as part of a proof?

The issue of the use of computers in a mathematical proof is fairly complex one. In the 70's two mathematicians solved a problem called the "four colour theorem" by reducing the problem to a finite (but very large) number of cases. They then used a computer to check all of these cases and claimed the theorem was proven. Can we count this as a mathematical proof?

Types of Proof:

In this section we are going to look at a number of different approaches to proof. The most straight forward is

Direct Proof:

Ex. Prove

$$\frac{1}{\sqrt{2-\sqrt{2}}}-\frac{1}{\sqrt{2+\sqrt{2}}}>\frac{1}{\sqrt{2}}.$$

Here are 4 attempts (only 2 of which are acceptable).

a) By the calculator, LHS = 0.7654..., RHS = 0.7071...
Therefore the result is true!

This is NOT an acceptable proof.

b)

This also is NOT a correct or valid proof. Notice that this 'proof' assumes the truth of the original statement IN the proof. Using this 'method' we can prove almost anything. For example, to 'prove' $1 = -1$, we simply square both sides and get $1 = 1$ whose truth certainly does not imply the first statement.

We can however modify the attempt in (b), and reverse the steps to write:

c)

Although valid, this proof is not very enlightening, since there are several steps which although correct are not obvious if one has not seen how they were arrived at. A much more straight forward proof is:

d) Let $x = \frac{1}{\sqrt{2-\sqrt{2}}} - \frac{1}{\sqrt{2+\sqrt{2}}}$. Note that $x > 0$.

Therefore $x = \frac{\sqrt{2+\sqrt{2}}-\sqrt{2-\sqrt{2}}}{\sqrt{2}}$ (common denominator), and so

$$x^2 = \frac{4-2\sqrt{2}}{2} = 2 - \sqrt{2} = \frac{2}{2+\sqrt{2}} > \frac{2}{2+2} = \frac{1}{2}$$

Therefore $x^2 > \frac{1}{2}$

Taking positive square roots we have $x > \frac{1}{\sqrt{2}}$.

Ex: Prove that

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

Ex: Prove that $\sqrt[8]{8!} < \sqrt[9]{9!}$.

Firstly note that this is equivalent to proving that $(8!)^9 < (9!)^8$.

From the definition $8! = 1.2.3...8 < 9^8$, therefore, $(8!)(8!)^8 < (8!)^8 9^8$ and so $(8!)^9 < (9!)^8$.

Generalisation:

We proved above the results: $\frac{1}{1000} - \frac{1}{1001} < \frac{1}{1000^2}$ and $\sqrt[8]{8!} < \sqrt[9]{9!}$.

These statements involved the specific numbers 8 and 1000, but there is nothing sacred about these, and in fact it is not hard to see that we can generalise these results to:

$$\text{For all } n \in \mathbb{Z}^+, \ \frac{1}{n} - \frac{1}{n+1} < \frac{1}{n^2}$$

and

$$\text{For all } n \in \mathbb{Z}^+, \ \sqrt[n]{n!} < \sqrt[n+1]{(n+1)!}$$

both of which are true statements.

These are examples of "for all statements". We use the symbol $\forall$ as shorthand for "for all". It is called a *universal quantifier*.

Ex. (From Calculus) $\forall x \in \mathbb{R}^+, e^x > 1 + x$.

Proof:

An "all" statement can sometimes be proved by splitting the problem into cases and consid-

ering each of these cases separately. This is called the method of **Proof by Exhaustion.**

Ex. $\forall x \in \mathbb{R}$, prove that $|x-3| \leq x^2 - 3x + 4$.

Ex. For all $n \in \mathbf{Z}$, prove that $n^3 \equiv n \bmod 6$.

"if...then" statements:

Many mathematical results can be stated in the form

'If P then Q', where P and Q are statements.

Ex: Suppose p is prime.
If $p \equiv 3 \bmod 4$ then it is impossible to write p as the sum of two integer squares.

Ex:
Suppose $a \in \mathbb{R}^+$.
If f is an odd function which is integrable on $[-a, a]$ then $\int_{-a}^{a} f(x)\ dx = 0$.

Ex. ('94 Nov)

Let $f : \mathbb{R} \to \mathbb{R}$ be a function. If f is an odd function then prove that $f(0) = 0$.

Ex. ('95 Nov)

Prove (by cases) that if n is a positive integer then $n^2 \equiv 0$ or $1 \bmod 4$.

Converses:

The **converse** of the statement

'If A then B', is 'If B then A'.

Note that the truth of the converse does NOT necessarily follow from the truth of the original statement.

For example, all numbers divisible by 4 are even, but the converse is false.

If and only if.... statements:

When a statement "If A then B" and its converse "If B then A" are both true, we often combine these two statements and write

"A if and only if B" or "A iff B".

Ex. An integer n is divisible by 6 iff it is divisible by 2 and 3.

Ex. $x \equiv 1 \bmod 4$ iff $x^3 \equiv 1 \bmod 4$.

Ex. A triangle is right-angled iff the square of the longest side equals the sum of the squares of the two shorter sides.

Proof: Suppose $\triangle ABC$ has a right-angle at A. Let Δ be the area of the triangle.

Consider the following construction:

$$\text{Area} = (b+c)^2 = b^2 + c^2 + 4\Delta \qquad \text{Area} = (b+c)^2 = a^2 + 4\Delta$$

$$\text{therefore } a^2 = b^2 + c^2.$$

Conversely, suppose $a^2 = b^2 + c^2$.

Construct a second triangle, right-angled at X with $XY = AB, ZX = AC$

$$YZ^2 = ZX^2 + YX^2 \quad (\text{by first part of the proof})$$
$$= AB^2 + AC^2 = c^2 + b^2 = a^2$$

Therefore $YZ = a$. Thus $\Delta XYZ \equiv \Delta ABC$ (SSS) and so $\hat{A} = \hat{X} = 90^o$.

"Some" Statements:

An existential generalisation or 'some' statement asserts that there exists something which satisfies a certain condition. We use the symbol $\exists$ as shorthand for 'there exists'. It is called the *existential quantifier*.

Ex. $\exists x \in \mathbb{R}$ such that $x^2 = 2$.

Ex. $\exists x \in \mathbb{R}$ such that $x > \pi$.

To prove a 'some statement', one method is to exhibit the object in question and show that it works.
This is called a **constructive** proof. Sometimes it is very difficult to actually produce the object whose existence we claim. In such a case it may however be possible to prove the existence of the object without necessarily producing it. This kind of proof is called a **non-constructive** proof.

Ex. Show that $a = 2^{1264504} - 1$ is not prime. That is, prove that there exists an integer k such that $k|a$.

Ex. Show that $f(x) = x^3 + 3x - 1$ has a zero between 0 and 1.
That is, show there exists a number a between 0 and 1 such that $a^3 + 3a - 1 = 0$.

Proof:

Observe that this is a non-constructive proof. (In fact $a = \sqrt[3]{\frac{\sqrt{5}+1}{2}} - \sqrt[3]{\frac{\sqrt{5}-1}{2}}$).

Ex. Prove that there exist $x, y \in \mathbb{R}$ such that

$$\begin{cases} 209x - 432y = -1 \\ 168x + 746y = 3 \end{cases}$$

Proof:

Observe that in the last two examples, the objects whose existence was claimed were in fact **unique**. We use the symbol $\exists!$ as an abbreviation for 'there exists a unique....'

Ex. Show $\exists! x \in \mathbb{R}$ such that $x^3 + 3x - 1 = 0$.

The existence was shown above. To show uniqueness, we note that if $f(x) = x^3 + 3x - 1$ then $f'(x) = 3x^2 + 3$ which is positive, and so the function is strictly increasing, and so can only take the value 0 once.

Ex: Given positive integers a and b prove $\exists! q, r \in \mathbf{Z}$ such that $a = qb + r$ with $0 \leq r < b$.

Ex: Show that if a square matrix A has an inverse, then the inverse is unique.

Multiple Quantifiers:

We have used the symbol $\forall$ to represent the universal quantifier and $\exists$ for the existential quantifier. Some mathematical statements involve more than one of these at a time.

For example, the statement, 'every positive real number has a real square root' can be translated into symbols as

$$\forall x \in \mathbb{R}^+ \quad \exists a \in \mathbb{R} \text{ such that } \quad a^2 = x.$$

Ex. $f : X \to Y$ is an onto function, means

$$\forall y \in Y \quad \exists x \in X \text{ such that } \quad y = f(x).$$

Note that the **order** of quantifiers is very important.

For example

$$\forall x \in \mathbb{N} \quad \exists y \in \mathbb{N} : x = y$$

is true, but

$$\exists y \in \mathbb{N} \quad \forall x \in \mathbb{N} : x = y$$

is false.

The definition of limits to infinity given is your Calculus course says: $\lim_{x\to\infty} f(x) = L$ means

$$\forall \epsilon > 0 \quad \exists N \in \mathbb{R} \text{ such that } \quad \forall x \in \mathbb{R}, \quad x > N \Rightarrow |f(x) - L| < \epsilon.$$

Ex: Prove from the definition that $\lim_{x\to\infty} \dfrac{x^2 - 1}{x^2 + 2} = 1$.

Ex. (Nov '94).
i) Show that if $x \in \mathbb{R}$ and $x > 1$ then $\sqrt{x+1} - \sqrt{x-1} < \frac{1}{\sqrt{x-1}}$.

ii) Prove that $\lim_{x\to\infty} \sqrt{x+1} - \sqrt{x-1} = 0$ from the definition

Ex. Prove that

$$\forall n \in \mathbb{Z}^+ \quad \forall m \in \mathbb{Z}^+ \quad \exists p \in \mathbf{Z}^+ \text{ such that } \frac{1}{m} + \frac{1}{n} > \frac{1}{p}.$$

Proof:

Negation:

The negation of a statement A is written as $\sim A$ (read as 'not A').

Clearly, $\sim A$ is true iff A is false.

The negation of $1 + 1 = 2$ is $1 + 1 \neq 2$.

The negation of $\frac{1}{n} - \frac{1}{n+1} < \frac{1}{n^2}$ is $\frac{1}{n} - \frac{1}{n+1} \geq \frac{1}{n^2}$.

Proof by Contradiction: (Reductio ad Absurdum).

A very common technique of proof which goes back to Euclid (and beyond ?) is the method of **Proof by Contradiction** also known by the latin name *Reductio ad Absurdum*. The method is to assume the negation of what we are trying to prove and obtain (if possible) a contradiction.

Ex. Prove that $8 + 31\sqrt{15} \neq 20\sqrt{41}$

Assume the contrary, i.e. assume $8 + 31\sqrt{15} = 20\sqrt{41}$.
Squaring both sides and simplifying, we get 3690240= 3690241 which is false, so the original proposition was true.

Ex. Prove that $\sqrt{2}$ is irrational.

Ex. Prove that $\log_2 3$ is irrational.

Ex. Prove that there are infinitely many primes.

Proof:
i) (Euclid) (Standard proof)

ii) (Kummer) Suppose not, then list them as $p_1, p_2, ..., p_n$ and let $N = p_1.....p_n$.

Now $N-1$ is a product of primes and so must have a prime factor p, in common with N. Thus $p|(N-(N-1))$, so $p|1$ which is impossible.

Ex. (Nov '95)

Use proof by contradiction to prove the following statement:

If a, b, c are positive integers with no common factor except 1, such that $a^2 + b^2 = c^2$, then exactly one of the numbers a or b must be even. (Hint: Work mod 4).

Contrapositives

The **contrapositive** of the statement "if A then B" is the statement "if not B then not A".

The contrapositive of a statement is logically equivalent to the original statement and so is true or false according as the original statement is true or false. It is often the case that proving the truth of the contrapositive is easier than proving the original statement.

Ex. Prove that if n^2 is even then n is even.

Ex. Prove that if $2^n - 1$ is prime then n is prime.

Ex. (Jun '93)
Let $n \in \mathbb{N}$ and let m be the smallest positive factor of n apart from 1. Show that m is prime.

Proof: The contrapositive says "if m, a factor of n, is composite, then n has a smaller factor than m.
$m = ab$, with a, $b \neq 1$, then $ab|n$, so a is a factor of n and $a < m$.

Negation of Multiple Quantifiers:

The negation of $\forall x P(x)$ is $\exists x(\sim P(x))$ and the negation of $\exists x P(x)$ is $\forall x(\sim P(x))$.

So, to negate a statement involving multiple quantifiers, we interchange all the $\forall$ symbols and $\exists$ symbols, and carefully negate the rest. Note especially that the negation of "if A then B" is "A and not B".

Ex. Negate:

$$\forall \epsilon > 0 \quad \exists \delta > 0 \qquad \text{such that} \quad \forall x \in (a-\delta, a+\delta) \quad |f(x) - f(a)| < \epsilon.$$

Ex. A set $S \subset \mathbb{R}$ is said to be **open** if

$$\forall x \in S \quad \exists \epsilon > 0 \quad \forall y \in \mathbb{R} \quad (\text{if } |x-y| < \epsilon \text{ then } y \in S).$$

Prove that $S = [1, 2)$ is **not** open.

The negation is

Proof:

2. Mathematical Induction:

Basic Principle of Induction:

Let $P(n)$ denote a proposition based on some natural number n.
For example, $P(n)$ might be the statement

$$1 + 2 + ... + n = \frac{1}{2}n(n+1).$$

$P(3)$ then denotes the statement $1 + 2 + 3 = \frac{1}{2}.3.4$

The **Principle of Induction** states that

i) If $P(n_0)$ is true for some $n_0 \in \mathbb{N}$ and

ii) whenever $P(k)$ is true (for some arbitrary $k \geq n_0$) it follows that $P(k+1)$ is true

then $P(n)$ is true for all integers $n \geq n_0$.

The Principle of Induction cannot be proven, (without assuming other equivalent axioms such as the Well-ordering principle). It is usually accepted as an axiom. The idea of mathematical induction seems to go back to Fermat/Pascal, although it is tacitly used whenever we say ".. and so on".

Ex: Prove the $16|(5^n - 4n - 1)$ for all $n \geq 1$.

Ex. Prove that

$$1^2 + 2^2 + ... + n^2 = \frac{1}{6}n(n+1)(2n+1).$$

Ex: (Nov, '94)
Prove $\exists N \in \mathbb{N}$ such that for $n > N, \quad n! > n^2$.

Strong Induction:

Some problems require a stronger version of induction.

For example, suppose we set out to prove the following statement using only ordinary induction:

Given the sequence $\{u_n\}$ with the properties:

$u_0 = 2, u_1 = 6 \qquad$ and $\qquad u_{n+2} = 6u_{n+1} - 8u_n, \quad \forall n \geq 0.$

Prove that $u_n = 4^n + 2^n$.

The statement is clearly true for $n = 0$ and if we suppose it true for some particular integer $k \geq 0$, then we can consider

$$u_{k+1} = 6u_k - 8u_{k-1}.$$

Now we can replace u_k with $4^k + 2^k$, which we assumed, but we CANNOT replace u_{k-1} with $4^{k-1} + 2^{k-1}$ since we did NOT assume the result true for $n = k - 1$. To correctly prove the result we would need to prove it true for $n = 1$ as well as $n = 0$ and assume it true for BOTH $n = k$ and $n = k - 1$, and then show it was also true for $n = k + 1$.

More formally, we need the strong (or extended) principle of induction which states that:

i) If $P(n_0), P(n_0 + 1), ..., P(n_0 + m)$ are all true for some $n_0 \in \mathbb{N}$ and for some $m \in \mathbf{Z}$, and

ii) whenever, for arbitrary $k \geq n_0 + m$, the truth of $P(n_0), P(n_0 + 1), ..., P(k)$ implies that $P(k + 1)$ is true,

then $P(n)$ is true for all integers $n \geq n_0$.

Ex. Fundamental theorem of arithmetic.

Every integer greater than 1 is the product of primes.

Ex: (Nov. '95)
Prove the following statement using induction.
The equation $3x + 5y = n$ has non-negative solutions x, y for all integers $n \geq 8$.

Proof: Let $P(n)$ be the above proposition for each integer n.

$P(8), P(9), P(10)$ are true since $8 = 5 + 3, 9 = 0.5 + 3.3, 10 = 2.5 + 0.3$

Suppose $P(n)$ is true for all integers $n = 8, 9, ..., k$. Thus $P((k+1)-3)$ is true (for $k \geq 10$), so $k + 1 - 3 = 3x^* + 5y^*$. Now $k + 1 = 3(x^* + 1) + 5y^*$ and thus $P(k+1)$ is true. Hence $P(n)$ is true for all integers $n \geq 8$ by induction.

(Note that the above problem can be done using ordinary induction by considering various cases.)

(If Time:) Method of Infinite Descent:

In induction, the key idea was to prove

$$P(k) \Rightarrow P(k+1).$$

The contrapositive of this is

$$\sim P(k+1) \Rightarrow \sim P(k) \text{ or } \sim P(k) \Rightarrow \sim P(k-1).$$

Thus, if one can show that $P(n)$ false implies $P(n-1)$ false for all $n > n_0$ and $P(n_0)$ true, then $P(n)$ must be true for all $n \geq n_0$. In a diagrammatic form:

$\bullet P(n)$ false
$\hookrightarrow \bullet P(n-1)$ false
$\hookrightarrow \bullet P(n-2)$ false
.....
.....
$\hookrightarrow \bullet P(n_0)$ false

but $P(n_0)$ is true, so $P(n)$ is true for all $n > n_0$.

This method is called the **Method of Infinite Descent** and appears to have been first used by Fermat.

Ex: Prove that $n^3 + 2n + 1$ is not divisible by 3 for any $n \in \mathbb{N}$.

Proof: Suppose that $3|(n^3 + 2n + 1)$ for some $n \in \mathbb{N}$. Now

$$(n-1)^3 + 2(n-1) + 1 = (n^3 + 2n + 1) + (-3n^2 + 3n - 3)$$

Therefore $3|((n-1)^3 + 2(n-1) + 1)$. But if $n = 1$, we have $3|4$ which is false, so by infinite descent we have that $n^3 + 2n + 1$ is not divisible by 3 for any $n \in \mathbb{N}$. (There is, of course, a

much easier way to do this problem!)

3. Logic and Truth Tables:

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 the moon is made of green cheese, then 1+1=3".
"The moon is made of green cheese"

We can conclude that $1 + 1 = 3$.

Note that the logic used here says nothing about the truth or falsity (here clearly the latter) of the statements involved. We are only saying that **if** the first two statements are true then the conclusion is true.

A **proposition** is a statement which is unambiguously true or false.

Logical Operators:

Given a collection of propositions we can build more complicated propositions using the following logical operators. Suppose p and q are propositions.

$\sim$	not	e.g	$\sim p$
$\wedge$	and	e.g	$p \wedge q$
$\vee$	or	e.g	$p \vee q$
$\rightarrow$	if....then	e.g	$p \rightarrow q$
$\leftrightarrow$	if and only if	e.g	$p \leftrightarrow q$
$\oplus$	exclusive or	e.g	$p \oplus q$

$p \wedge q$ is sometimes called the **conjunction** of p and q, while $p \vee q$ is called the **disjunction** of p and q.

Observe that $q \rightarrow p$ is the converse of $p \rightarrow q$ and $(\sim q) \rightarrow (\sim p)$ is the contrapositive of $p \rightarrow q$.

Because our propositions are always either true or false, we can calculate the truth value of our compound propositions by knowing the truth values of the constituent components. We study this, by writing down all the possible cases using **truth tables**.

The truth table for implication is a little more tricky. One way to see it is to consider the statement, "Be quiet or I'll kick you out". (Note that 'Be quiet' is not a proposition, but we can think of this as the same as 'You are quiet'.) In ordinary English usage, this is equivalent to saying "If you are not quiet then I'll kick you out". Thus, the truth table of $p \to q$ should be the same as that for $\sim p \vee q$, i.e.

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

Similarly, recalling that $p \leftrightarrow q$ is equivalent to $(p \to q) \ \wedge \ (q \to p)$, we have the truth table:

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

Ex. Prove that

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

have the same truth value.

A compound proposition that is always true, regardless of the truth values of the constituent propositions, is called a **tautology**. A compound proposition that is always false, regardless of the truth values of the constituent propositions, is called a **contradiction**. A compound proposition that is neither a tautology nor a contradiction, is called a **contingency**.

We use the letter t to denote the proposition that is always true and c to denote the proposition that is always false.

For example, $p \wedge (\sim p)$ is a contradiction, while $p \vee (\sim p)$ is a tautlogy.

Ex. (June '90).
S is the proposition $\sim p \to ((p \to q) \wedge \sim q)$. Construct a truth table for S. Is S a tautlogy? State the converse of S

Ex. (Nov. '95)
Consider the compound proposition

$$[(p \wedge q) \vee (\sim q)] \to ((\sim q) \to p).$$

What truth values for p and q will make the proposition false?

Ex. Show that $[(\sim p \to \sim q) \wedge \sim p] \wedge q$ is a contradiction.

Propositions which have the same truth values are said to be **logically equivalent**. We denote this by writing $P \Longleftrightarrow Q$. That is,

$$P \Longleftrightarrow Q \qquad \text{means} \qquad P \longleftrightarrow Q \qquad \text{is a tautology.}$$

So if a compound proposition P is a tautology, we have $P \Leftrightarrow t$, and if it is a contradiction then $P \Leftrightarrow c$.

Ex.$\sim (p \wedge q) \Longleftrightarrow \sim p \vee \sim q$.

We can make a list of the more well-known simple equivalences

1.	$p \wedge q \Longleftrightarrow q \wedge p$	$p \vee q \Longleftrightarrow q \vee p$	commutative law
2.	$(p \wedge q) \wedge r \Longleftrightarrow p \wedge (q \wedge r)$	$(p \vee q) \vee r \Longleftrightarrow p \vee (q \vee r)$	associative law
3.	$p \wedge (q \vee r) \Longleftrightarrow (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \Longleftrightarrow (p \vee q) \wedge (p \vee r)$	distributive law
4.	$p \wedge t \Longleftrightarrow p$	$p \vee c \Longleftrightarrow p$	identity
5.	$p \vee \sim p \Longleftrightarrow t$	$p \wedge \sim p \Longleftrightarrow c$	negation
6.	$\sim (\sim p) \Longleftrightarrow p$		double negative
7.	$p \wedge p \Longleftrightarrow p$	$p \vee p \Longleftrightarrow p$	idempotent
8.	$\sim (p \vee q) \Longleftrightarrow \sim p \wedge \sim q$	$\sim (p \wedge q) \Longleftrightarrow \sim p \vee \sim q$	De Morgan
9.	$p \vee t \Longleftrightarrow t$	$p \wedge c \Longleftrightarrow c$	domination

You should compare these laws of logical equivalence with the laws of set theory earlier in this course. There is an obvious correspondence between $\wedge$ and $\cap$, and $\vee$ with $\cup$. There is also a principle of duality in operation here.

Ex: Use the laws of logical equivalence to simplify

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

Ex. Prove that $\sim (p \vee (\sim p \wedge q)) \Longleftrightarrow \sim p \wedge \sim q$.

In propositions involving the implication symbol, we replace $p \to q$ with $\sim p \vee q$.

Ex. Show that $(q \to p) \to (p \wedge q) \Longleftrightarrow q$.

Ex. Show that $\sim (p \to q) \Longleftrightarrow p \wedge (\sim q)$.

Ex. Prove that $\sim (p \to q) \to [(q \vee r) \to (p \vee r)] \iff t$.

Note that **all** logical connectives can be written in terms of $\sim$ and $\vee$.
Viz: $\sim p, p \vee q, p \wedge q \Leftrightarrow \sim (\sim p \vee \sim q), p \to q \Leftrightarrow \sim p \vee q$ and so on.

We say that the set $(\sim, \vee)$ is **functionally complete.**

Rules of Inference:

Consider the 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."

The form of argument here is

$$\begin{array}{c} p \to q \\ p \\ \hline q. \end{array}$$

Such an argument is called a **rule of inference**, and is valid because the conclusion (the last line) is true provided that the **hypotheses** are true.

This particular rule of inference is commonly called **modus ponens**.

Observe that the following is **not** valid:

$$\begin{array}{c} p \to q \\ q \\ \hline p. \end{array}$$

For example, if we let p = "I live in Queensland" and q= "I live in Australia" then the above is clearly not correct.

Another rule of inference, known as **modus tollens** is:

$$\frac{\begin{array}{c} p \to q \\ \sim q \end{array}}{\sim p.}$$

The hypothetical syllogism is:

$$\frac{\begin{array}{c} p \to q \\ q \to r \end{array}}{p \to r.}$$

The disjunctive syllogism is:

$$\frac{\begin{array}{c} p \vee q \\ \sim p \end{array}}{q.}$$

and the simplification syllogism is:

$$\frac{p \wedge q}{p.}$$

Note that a syllogism

$$\frac{\begin{array}{c} P_1 \\ P_2 \\ . \\ . \\ . \\ P_r \end{array}}{Q.}$$

is valid is the same as saying

$$P_1 \wedge P_2 \wedge P_3 \wedge ..... \wedge P_r \Longleftrightarrow Q$$

or

$$P_1 \wedge P_2 \wedge P_3 \wedge ..... \wedge P_r \longleftrightarrow Q$$

is a tautology.

Proof by Contradiction:

This is achieved by the following syllogism:

$$\frac{\sim p \to c}{p.}$$

since $(\sim p \to c) \longleftrightarrow p$ is a tautology.

Ex. Prove that

$$\begin{array}{c} \sim q \to p \quad (1) \\ q \to r \quad (2) \\ \sim r \quad (3) \\ \hline p. \end{array}$$

is valid

Proof:

$\sim r$	(3)
$\sim q$	(2) with m.t.
$p.$	(1) with m.p.

Ex. Prove that

$$\begin{array}{c} p \to r \quad (1) \\ r \to \sim s \quad (2) \\ q \to s \quad (3) \\ \hline p \to \sim q. \end{array}$$

is valid

Proof:

suppose p	
r	(1) with m.p.
$\sim s$	(2) with m.p.
$\sim q$	(3) with m.t.
$p \to \sim q.$	

Ex. Prove that

$$\begin{array}{c} \sim p \\ r \to p \\ \sim q \vee r \\ \hline \sim q. \end{array}$$

is valid

Ex. Prove that

$$\begin{array}{c} p \\ p \to q \\ \sim q \vee \sim r \\ \hline \sim r. \end{array}$$

is valid

Ex. Prove that

$$\frac{\begin{array}{c} p \wedge \sim q \\ p \to r \\ s \to q \end{array}}{r \wedge \sim s.}$$

is valid

Ex. Prove that

$$\frac{\begin{array}{c} p \to q \\ (q \wedge s) \to t \\ s \wedge p \end{array}}{t.}$$

is valid

One can give a direct or an indirect proof of this last example.

Word Problems:

Ex. Either Moriarty has escaped or the money is missing.
If Mr. Smith is not dead then Moriarty has not escaped.
Either the money is not missing or Mr. Smith is dead
Therefore, Mr. Smith is dead.

Using the symbols e= 'Moriarty has escaped', d= 'Mr. Smith is dead, m= the money is missing', this translates to

$$\begin{array}{c} e \vee m \\ \sim d \rightarrow \sim e \\ \sim m \vee d \\ \hline d. \end{array}$$

which is valid.