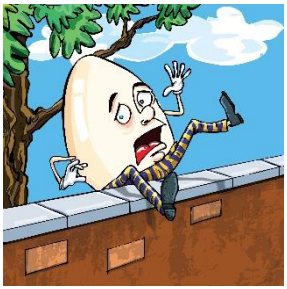
1. LOGIC



There existed an egg who sat on a wall,
And the wall being short implies this story is tall.
Now if that fat egg had had a great fall
Or slipped off the top, but not jumped, then not all
The king's horses and all the king's men,
If they worked through the day and the evening, then
They could not succeed if and only if when
They attempted to put Humpty together again.

§1.1. The Role of Logic in Mathematics

Over many hundreds of years mathematics has played a vital role in the development of the sciences and so it is often regarded as a science itself. But mathematics is quite different to any of the other sciences in one important respect. It has no empirical facts. Physicists carry out experiments and formulate hypotheses. They use mathematics as a language to describe their hypotheses and as a tool to explore their logical consequences. But in the final analysis physical theories must be supported by experimental facts.

Where mathematics appears to come closest to being an experimental science is in geometry. We measure the angles of a triangle and they appear to total 180°. But when we do that we're acting as experimental physicists. We now know that there's no logical necessity

for the sum of the angles of a triangle to be 180°. While this *is* a fact in Euclidean geometry, the geometry we all learnt at school, there are other logically consistent geometries where this is not the case. Could it not be that the angles of a triangle add up to slightly more than 180° or a little less. Perhaps the discrepancy is so minute that it hasn't yet been detected in our measurements. Who's to say whether Euclidean geometry is the right one to describe physical space? Only a physicist could do this with careful measurement – certainly not a mathematician.

In a very real sense, mathematics has no facts. It is concerned with the logical relationships *between* facts. Well then, is mathematics just the same as logic? No. Logic provides the tools for reasoning. Mathematics uses these logical tools to construct elaborate systems which can be used by science as models for different aspects of the real world.

If mathematics was to be viewed as a science, and there are those who argue that it should be, then its laboratory is the human mind. Its instruments are the techniques of proof. This is why it is important for anyone studying mathematics to have an appreciation of logic.

§1.2. The Role of Logic in Computing Science

What was said about logic in mathematics is also true of computing science because in theoretical computer science there are theorems and proofs just as in

mathematics. In fact there are those chauvinist mathematicians who dismiss theoretical computer science or theoretical physics as just particular branches of mathematics!

In one sense they're right. But computer science and theoretical physics are sufficiently integrated with experimental and practical aspects that for practical purposes they are quite properly studied in their own specialised departments. However you should never forget that the boundary between theoretical computing science and discrete mathematics is somewhat arbitrary. There's really a continuum that takes us all the way from mathematics to computer science and back again.

So, just as logic is important to mathematics, it is important to computer science. But for computer scientists, logic plays another very important role which affects some of the most applied areas of that subject.

It is no accident that at the heart of the central processing chip there is the 'arithmetic logic unit'. We talk about the logic of computer programs, for very good reasons. At a higher level still, to understand the theory of databases one needs to understand logic, and its partner, set theory. And another area, of interest to both mathematicians and computing scientists alike, is the area of automated theorem proving and proofs of program correctness.

§1.3. Propositions and Truth Functions

A **proposition** is a statement for which it is meaningful to say that it is true or false (but not both).

The **truth value** of a proposition *p* is T or F according as the proposition is false or true.

T = TRUE F = FALSE

Now we don't need to ask the deep question "what is truth?" For our purpose truth values can be thought of as tags that are given to certain statements. Logic is concerned with *relative* truth, that is, the truth of a compound statement given the truth of its primitive constituents and the truth of those primitive statements is established by other means, or is simply assumed in axioms or definitions.

Example 1

"It rained today" is a proposition while "Will it rain today?" or "Come inside, it's raining." are not.

Some statements appear to be propositions, but on closer examination they are not because to attach a truth value to them leads to a logical paradox.

Example 2

THIS STATEMENT IS FALSE

is not a proposition because if we say that it is true then it is false and if we say that it is false then it is true.

It is the self-referential nature of this statement, the fact that it purports to be saying something about itself, which appears to cause the problem. However there are cases, involving no self-referentiality, that still lead to trouble.

Example 3

Consider the following infinite list of statements:

AT LEAST ONE OF THE FOLLOWING STATEMENTS IS FALSE
AT LEAST ONE OF THE FOLLOWING STATEMENTS IS FALSE
AT LEAST ONE OF THE FOLLOWING STATEMENTS IS FALSE
.....……
…….

There is no self-referentiality here. Each statement purports to be saying something about all the remaining ones. So, although each reads identically to the next, they are all different statements, referring to a different set of statements, and so they don't all have to have the same truth value.

But if any one of them is false then all the remaining ones are true and it's easy to see that this leads to a contradiction. But if they're all true we again get a contradiction. Think this out carefully. If it is false that all the following statements are false then one of the following statements must be true!

Such problems can keep a logician awake at night, but we take the more practical view that we'll ignore such potential problems and hope that we never meet them. That is a reasonable practical attitude because such logical paradoxes only exist in the logic laboratory. One has to go out of one's way to produce them.

§1.4. Compound Propositions

Compound propositions can be made up from simpler ones in such a way that their truth value can be determined from those of their constituents. We use **truth tables**. These set out the truth value of compound statements based on the truth values of their constituents. Note that you don't need to know what the statements are – just whether they are true or false. If *p* is TRUE and *q* is FALSE then *p* and *q* is FALSE while *p* or *q* is TRUE.

Not, And, Or

The simplest truth operator is **not** which only involves one constituent. Its truth table is:

p	**not p**
T	F
F	T

The truth tables for **and** and **or** are:

p	q	p and q
T	T	T
T	F	F
F	F	F
F	T	F

p	q	p or q
T	T	T
T	F	T
F	T	T
F	F	F

Notice that "*p* or *q*" is defined to be TRUE even when both are true. Sometimes in everyday English we use "or" in an exclusive sense, but in logic, and in mathematics, it always includes the possibility of both.

Richard Feynman, a famous physicist, was once asked by the Dean's wife at Princeton University whether he wanted milk or lemon in his tea. He replied "both". "Surely you're joking Mr Feynman." He was, but he was making a point about the mathematician's use of the word 'or' – it *can* include both.

In order to work at the level of the underlying logical structure we denote primitive propositions (ones which are not built up from simpler ones) by letters of the alphabet just as in algebra we represent numbers by letters.

The above three truth operators are denoted by special symbols –, $\wedge$, $\vee$ respectively.

$-p$ denotes 'not *p*';

$p \wedge q$ denotes '*p* and *q*';

$p \vee q$ denotes '*p* or *q*';

Several variations are in common use: 'not *p*' is often denoted by p' , $\neg p$, or $\bar{p}$. Sometimes 'p and q' is denoted by p.q and 'p or q' can be written as p + q.

Example 4

$(p \vee q) \wedge -(p \wedge q)$ denotes the compound statement '*p* or *q* but not both'. This is the 'exclusive or'. Also note the use of the word "but" here. It is simply an alternative to 'and'. While there may be overtones of contrast or emphasis with 'but' that we don't get with 'and', at the fundamental level of logic their meaning is identical.

Implication

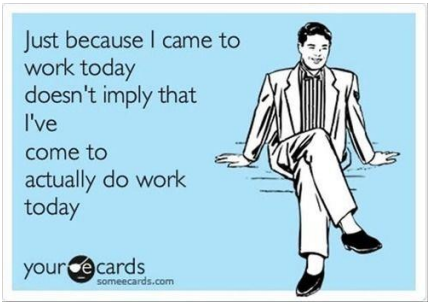
Our next truth operator is one that's very much misunderstood – implication. The definition of '*p* implies *q*' is given by its truth table:

p	***q***	***p* implies *q***
T	T	T
T	F	F
F	T	T
F	F	T

The problem that many people have with this definition is the third row which says that a false proposition implies a true one! In fact all it shows is that the technical definition of implication differs somewhat from the ordinary sense of the word. In normal usage implication involves a causal connection. It might be the case that I'm wealthy and that I'm honest. In the ordinary sense of the word we wouldn't say however that "being wealthy implies that I am honest". Wealth does not cause honesty. However if both propositions are true for me

then, in the sense of propositional logic, “I am wealthy” implies “I am honest”.

Because propositional logic deals with isolated propositions it can’t express the notion of wealthy people *always* being honest (or its negation). That requires quantifiers’, something we’ll discuss later.



If you still feel uneasy about the above definition of implication you might like to ask yourself how else you might define it. For example if you decide that false statements can’t imply anything then you would want to change the last two rows of the truth table to become:

p	**q**	
T	T	T
T	F	F
F	T	F
F	F	F

But this is just the truth table for ‘and’ and surely ‘implies’ doesn’t mean the same as ‘and’. The final vindication for the accepted definition however only comes when we see implication in the context of quantifiers (see §1.8).

Notation: We denote 'p implies q' by $p \to q$.
Sometimes this is written as $p \Rightarrow q$ or $p \supset q$.

Equivalence

We say that p is (logically) **equivalent to** q if they have the same truth value.

We'll denote 'p is equivalent to q' by $p \leftrightarrow q$. Other notations in use are $p \equiv q$ and $p \Leftrightarrow q$.

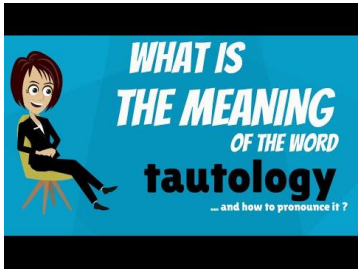
This definition can be set out in a truth table:

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

Summary of Truth Operators

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \to q$	$p \leftrightarrow q$
T	T	F	T	T	T	T
T	F	F	F	T	F	F
F	T	T	F	T	T	F
F	F	T	F	F	T	T

§1.5. Tautologies



A **tautology** is a proposition built up from primitive propositions, which is always true irrespective of the truth values of the constituent propositions.

Tautologies are logical theorems. For example

"(p and q) implies (q and p)" doesn't give us any information about the statements p and q. Rather it tells us about the symmetry of the "and" operator.

Example 5: The following three propositions are tautologies:
(1) $p \leftrightarrow p$
(2) $p \rightarrow (p \vee q)$
(3) $(p \wedge q) \leftrightarrow (q \wedge p)$
But $(p \vee q) \rightarrow (p \wedge q)$ is not a tautology.

The above tautologies seem intuitively obvious. More complicated statements could be very difficult to test. However any proposition can be tested mechanically to determine whether or not it is a tautology. We use a 'truth table', where all possibilities are considered.

Example 6: Is "$-(-p \vee -q) \leftrightarrow p \wedge q$" a tautology?
We consider each of the four possible combinations of truth values (with a proposition involving p, q and r there are eight combinations) and work out the resulting truth value of the whole statement.

A very compact way of setting this out is in a table where each row corresponds to one such combination. We write the truth values for the primitive statements p and q underneath those symbols and the truth values for each sub-proposition underneath the symbol for the relevant operator.

−(	**−**	**p**	**∨**	**−**	**q)**	**↔**	**p**	**∧**	**q**
T	F	T	F	F	T	T	T	T	T
F	F	T	T	T	F	T	T	F	F
F	T	F	T	F	T	T	F	F	T
F	T	F	T	T	F	T	F	F	F
9	5	1	8	6	2	10	3	7	4

The last row isn't usually included. It's given here simply to show the order in which the columns were filled in. This order can be varied a little but, for example, the first column cannot be filled in until the ∨ column (representing the proposition to be negated) has been completed.

§1.6. Translating From English

***p* → *q* might be expressed as:**

if *p* then *q*
p implies *q*
q is implied by *p*
q, if *p*
p only if *q*
p is a sufficient condition for *q*
q is a necessary condition for *p*

***p* ↔ *q* might be expressed as:**

p is equivalent to *q*
p if and only if *q* (sometimes this is abbreviated to "*p* iff *q*")
p is a necessary and sufficient condition for *q*

$p \wedge q$ might be expressed as:

p and q
not only p, but q

$p \vee q$ might be expressed as:

p or q
unless p then q
p, unless q
at least one of p and q

Miscellaneous constructions:

p but not q	$p \wedge -q$
neither p nor q	$-(p \vee q)$
p or q but not both	$(p \vee q) \wedge -(p \wedge q)$
	or more simply as $p \leftrightarrow -q$

[To see that these are equivalent use a truth table.]

§1.7. Laws of Logic

The following is a list of tautologies that are commonly used. Most of them are intuitively obvious but all of them can be tested using truth tables. Examine them, think about them, but *do not attempt to learn the list*.

To avoid complexity we use the convention that there are implied parentheses around each side of an implication or an equivalence and we assume that the negation operator only applies to the following proposition. If we wish to express something different then we need to include parentheses.

For example $p \vee q \leftrightarrow r$ means (p $\vee$ q) $\leftrightarrow r$. If we wish to express $p \vee (q \leftrightarrow r)$ then the parentheses are needed. Also $-p \wedge q$ means $(-p) \wedge q$. If we wish to express $-(p \wedge q)$ we need the parentheses.

Commutative Laws:

(1) $p \vee q \leftrightarrow q \vee p$
(2) $p \wedge q \leftrightarrow q \wedge p$

Associative Laws:

(3) $(p \vee q) \vee r \leftrightarrow p \vee (q \vee r)$
(4) $(p \wedge q) \wedge r \leftrightarrow p \wedge (q \wedge r)$

Distributive Laws:

(5) $p \wedge (q \vee r) \leftrightarrow (p \wedge q) \vee (p \wedge r)$
(6) $p \vee (q \wedge r) \leftrightarrow (p \vee q) \wedge (p \vee r)$

Idempotent Laws:

(7) $p \vee p \leftrightarrow p$
(8) $p \wedge p \leftrightarrow p$

De Morgan Laws:

(9) $-(p \vee q) \leftrightarrow -p \wedge -q$
(10) $-(p \wedge q) \leftrightarrow -p \vee -q$

Miscellaneous Laws:

(11) $p \wedge q \rightarrow p$
(12) $p \rightarrow p \vee q$

(13) $-(-p) \leftrightarrow p$

(14) $p \vee -p$

(15) $-(p \wedge -p)$

These last two assert that a proposition must either be true or false but not both.

Syllogism:

(16) $(p \rightarrow q) \wedge\ p \rightarrow q$

A *syllogism* is a logical argument of the form:

$p \rightarrow q$

But p.

Therefore q.

Proof by Contradiction:

(17) $(p \rightarrow q) \wedge -q \rightarrow -p$

Example 7

"If you'd left the keys on the table they'd still be there. But the keys aren't there so you couldn't have left them there." which analyses formally to:

p = "You left your keys on the table."

q = "The keys are still there."

If p then q. But not q. Therefore not p.

(Of course there are hidden assumptions such as "nobody else has come in" and "keys cannot spontaneously evaporate").

Transitive Property of Implication:

(18) $(p \rightarrow q) \wedge\ (q \rightarrow r) \rightarrow (p \rightarrow r)$

Note how the parentheses around $p \to r$ are necessary. A construction such as $p \to q \to r$ is ambiguous since implication is not associative.

§1.8. Quantifiers

A **predicate** is a statement that involves variables. Predicates become propositions when particular objects (e.g. numbers) are substituted for the variables. The resulting propositions have truth values that depend on those elements.

An ***n*-ary predicate** is one which applies to a combination of n elements. Special terms are **unary** if $n = 1$, **binary** if $n = 2$ and **ternary** if $n = 3$. A **unary** predicate is what we usually think of as a **property**, such as 'x is even' or 'x is female'. We could write these symbolically as Ex for 'x is even' and Fx for 'x is female'. There must be some underlying set over which the variables range. In the case of E it might be the set of integers and in the case of F it might be the set of all students in a particular class.

A **binary** predicate is what we usually think of as a relation, such as '$x < y$' or 'x has passed y'. We could write these symbolically as xLy for '$x < y$' and xPy for 'x has passed the course y'. The first of these example might have x and y ranging over the set of integers and the second example might have x ranging over the set of students in a particular class and y ranging over the courses at a particular university.

Example 8
'x is even' is a unary predicate that is TRUE for $x = 2$ and FALSE for $x = 3$.
'x loves y' is a binary predicate involving two elements x and y from a set of people.
If x = Romeo and y = Juliet then this becomes a true statement.
'x is the distance between P and Q' is a ternary predicate involving a combination of a number and two points.

Notation: We commonly denote predicates by upper case letters and the variables by lower case letters. Often the variable names follow the predicate name such as Pn, Qxy and Rabc. But in the case of a binary predicate it's more usual to put one element on each side of the predicate name as in xRy. This what we usually do in mathematics with predicates such as '=' and '<'.

If P is a unary predicate then $\forall \boldsymbol{x}\ \mathbf{P}\boldsymbol{x}$ means 'for all x, Px (is true)' and $\exists \boldsymbol{x}\ \boldsymbol{P}\boldsymbol{x}$ denotes 'for some x, Px', or 'there exists x such that Px'. 'For all' is called the **universal quantifier** and 'for some' is called the **existential quantifier**.

NOTES:
(1) 'Some' means 'at least one'. Even if Px is true for just one x we're entitled to claim that $\exists x$ Px.

(2) There is some assumed non-empty universe over which we are quantifying.

(3) The variable "bound" by a quantifier is a "dummy" variable and can be replaced by another provided this is done consistently throughout the scope of the quantifier. This means that $\forall x(Px \rightarrow Qx)$ is equivalent to $\forall t(Pt \rightarrow Qt)$ or $\forall w(Pw \rightarrow Qw)$. This is analogous to the dummy variable of integration in a definite integral and to local variables in many computing languages.

(4) When working with quantifiers "Px impliesQx" usually has an implied universal quantifier and should be translated as $\forall x(\mathrm{P}x \rightarrow \mathrm{Q}x)$. It is for this reason that implication is defined to be true when the "antecedent" is false. The statement $\forall x(x$ is even $\rightarrow x^2$ is even) has to be true for *all* integers, including odd ones. The definition of implication makes it "vacuously true" in the case of odd integers.

(5) In normal language 'implies' often has causal overtones, but in logic this is not the case. The statement "I am male implies that I am intelligent" might seem to be saying that being male predisposes someone to be

intelligent, or even that men are more intelligent than women. But if you are female, whether or not you are intelligent, the statement of implication is true.

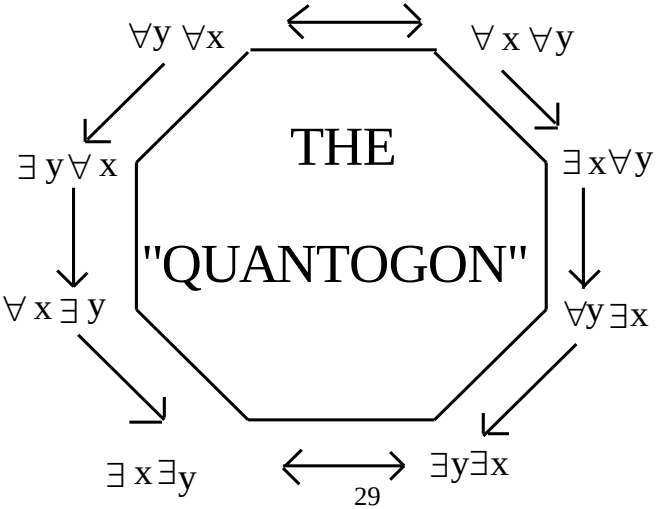
Suppose that in a survey of 100 men, all who eat red meat have good eyesight. A medical researcher might begin to investigate whether this is a coincidence, whether red meat is good for eyesight, whether good eyesight predisposes someone to eat red meat, or whether there is some other factor that causes both good eyesight and a liking for red meat. For a logician the work is done.

For the sample in question the assertion:

$\forall m$ (m eats red meat $\rightarrow$ m has good eyesight)

is true.

With a predicate involving two variables there are eight ways they can be quantified: each of x, y can be quantified by $\forall$ or $\exists$ and they can be quantified in either order. The logical relationships between them are displayed by the following diagram:



Note

carefully the difference between $\exists x \forall y$ and $\forall y \exists x$. The first is the stronger of the two. It implies the second but not conversely. For example $\exists x \forall y [x > y]$ claims that there's an integer larger than every integer (FALSE) while $\forall y \exists x [x > y]$ makes the weaker (TRUE) claim that for every integer there's a larger one.

If xLy means 'x loves y' (within an appropriate universe) $\forall y \exists x [xLy]$ makes the claim that "nobody is unloved" while $\exists x \forall y [xLy]$ comes close to making the religious claim "God loves everybody".

The definition of limits in calculus makes subtle use of quantifiers. The statement that "the limit of $f(x)$ as $x \to a$ is b" is defined as:

$$\forall \varepsilon \, \exists \delta \, \forall x \, [(\varepsilon > 0) \wedge (0 < |x - a| < \delta) \to (|f(x) - b| < \varepsilon)].$$

If we interchanged the first two quantifiers we would get the stronger statement:

$$\exists \delta \, \forall \varepsilon \, \forall x \, [(\varepsilon > 0) \wedge (0 < |x - a| < \delta) \to (|f(x) - b| < \varepsilon)].$$

which, in effect, claims that $f(x) = b$ for all x in some region about $x = a$.

§1.9. Quantifiers in Mathematics

Suppose that the universe of quantification is $\mathbb{N} = \{0, 1, 2,...\}$, the set of natural numbers and that the primitive predicate is $x = y$, supplemented by the functions of addition and multiplication. Other predicates can be built up from these as follows:

x is prime	$(x \neq 1) \wedge \forall y\,[y \text{ divides } x \rightarrow$
$x \neq y$	$\neg(x = y)$ $(y = 1) \vee (y = x)]$
x is even	$\exists y\,(x = 2y)$ $\exists y.(x = 2y)) \wedge \forall y\,\exists q[x = yq \rightarrow$
$x \leq y$	$\exists z\,(y = x + z)$ $(y = 1) \vee (y = x)]$
$x < y$	$(x \leq y) \wedge (x \neq y)$
x is a prime power	$\exists p[p \text{ is prime} \wedge \forall q[(q \text{ is prime}) \wedge$ i.e. $\exists z\,(y = x + z) \wedge \neg(x = y)$ $(q \text{ divides } x) \rightarrow (q = p)]]$
x divides y	$\exists z\,(y = xz)$

These last two statements can be expanded until they are expressed entirely in terms of equality, addition and multiplication.

The famous *Goldbach Conjecture* (whose truth is strongly suspected but has never been proved) asserts that "every even number bigger than 2 is the sum of two primes". This can be written as:

$$\forall x\,[(x > 2) \wedge (x \text{ is even}) \rightarrow \exists y\,\exists z[(y \text{ is prime}) \wedge (z \text{ is prime}) \wedge (x = y + z)]$$

§1.10. Negation Rules

To prove a theorem by contradiction requires the negation of the theorem to be assumed in order to reach a contradiction. If the statement has a complicated logical structure it may be necessary to rewrite this negation more simply. One can do this by using the following

rules describing the way negation interacts with the other truth operators and the two quantifiers.

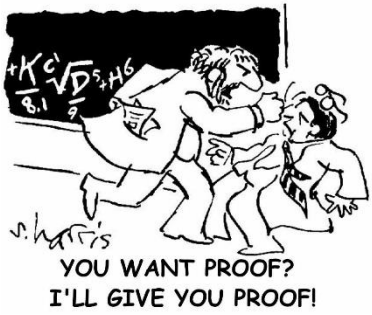
PROPOSITION	NEGATION
$-p$	p
$p \wedge q$	$-p \vee -q$
$p \vee q$	$-p \wedge -q$
$p \rightarrow q$	$p \wedge -q$
$p \leftrightarrow q$	$p \leftrightarrow -q$
$\forall x Px$	$\exists x -Px$
$\exists x Px$	$\forall x -Px$

Example 9

The negation of $\exists x[Px \rightarrow (Qx \wedge -Rx)]$ is

$$
\begin{aligned}
-\exists x[Px \rightarrow (Qx \wedge -Rx)] &\leftrightarrow \forall x -[Px \rightarrow (Qx \wedge -Rx)] \\
&\leftrightarrow \forall x\, [Px \wedge -(Qx \wedge -Rx)] \\
&\leftrightarrow \forall x[Px \wedge (-Qx \vee - -Rx)] \\
&\leftrightarrow \forall x[Px \wedge (-Qx \vee Rx)].
\end{aligned}
$$

§1.11. Writing Proofs



A proof is a *chain of reasoning* that leads from a set of assumptions to a conclusion. There are many proofs in computing science and, of course, mathematics is all theorems and proofs, or so it seems.

The important word here is ‘chain’. A proof is not just a heap of arguments which make the conclusion seem plausible. A case for the prosecution in a court of law might rely on evidence heaped upon evidence till the scales of justice tip. In a proof, however, we present a chain — an intellectual journey. Whoever takes this journey should find that the truth of what is being proved is inescapable.

Structure is as important in a proof as it is in a computer program. No trained computer programmer would dream of writing a program by assembling some loosely connected statements in some arbitrary order. Yet that is what the same programmer often does when asked to write a proof.

The structure of a proof must reflect the logical structure of the proposition being proved. If you keep this in mind then many simple proofs just seem to write themselves with little or no imagination required on the part of the prover. In fact this approach is built in to automated theorem-proving software. These programs are not designed to put mathematicians out of a job. A really significant mathematical break-through will always require the mathematical ingenuity of a real mathematician. But there is a growing area of proof of program correctness, whereby a computer program is analysed logically in a mechanical way and a proof that it meets the specifications is generated.

§1.12. Patterns of Proof

IMPLICATION: p → q
We assume *p* and then prove *q*.

p → q
Suppose *p*
……
Therefore *q*

Example 10: Prove that if n is odd then n^2 is odd.
Proof: Suppose *n* is odd.
Then $n = 2k + 1$ for some integer *k*.
Thus $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, which is odd.

NEGATION: −p
If the statement of the theorem has a negative form it is usually best to use Proof by Contradiction.

−p
Suppose *p*.
……
A contradiction.
Hence −*p*.

Example 11: Prove that $\sqrt{2}$ is irrational.
Proof: Suppose that $\sqrt{2}$ is rational. Therefore $\sqrt{2} = m/n$ for some integers *m*, *n* with $n \neq 0$.
We may suppose without loss of generality (wlog) that *m*, *n* have no common factor (i.e. are coprime). Now $m^2 =$

$2n^2$ and so m is even. Put $m = 2k$. Then $4k^2 = 2n^2$ and so $n^2 = 2k^2$ which implies that n is even. This contradicts the assumption that m, n are coprime.
Hence $\sqrt{2}$ must be irrational.

Example 12: Prove that:

$$\forall x\, \exists y\, [(Px \to -Qy) \to (Qx \to -Px)]$$

This is a tautology, that is, it is true for all possible predicates P, Q.

Proof: We suppose that the theorem is false and use the Negation Rules.

Suppose $-\forall x\, \exists y\, [(Px \to -Qy) \to (Qx \to -Px)]$.

$\therefore\ \exists x\, -\exists y\, [(Px \to -Qy) \to (Qx \to -Px)]$.

$\therefore\ \exists x\, \forall y\, -[(Px \to -Qy) \to (Qx \to -Px)]$.

$\therefore\ \exists x\, \forall y\, [(Px \to -Qy) \wedge -(Qx \to -Px)]$.

$\therefore\ \exists x\, \forall y\, [(Px \to -Qy) \wedge Qx \wedge --Px)]$.

$\therefore\ \exists x\, \forall y\, [(Px \to -Qy) \wedge Qx \wedge Px)]$.

In particular, taking $y = x$ we get:

$(Px \to -Qx) \wedge Qx \wedge Px)$ which is a contradiction.

Hence the original proposition is true.

OR: $\mathbf{p \vee q}$

The simplest way to prove a 'p or q' theorem is to write it as $-p \to q$. **Note:** $(p \vee q) \leftrightarrow (-p \to q)$ is a tautology.

$\mathbf{p \vee q}$

Suppose $-p$.

……..

Therefore q.

Hence $p \vee q$.

Example 13: Prove that there exists an irrational number x such that $x^{\sqrt{2}}$ is rational.
This doesn't appear to have an obvious 'p or q' form. But if we start the proof with "let $x = \sqrt{2}$ or $x = (\sqrt{2})^{\sqrt{2}}$" then our goal is to prove that, for one of these alternatives, x is irrational and $x^{\sqrt{2}}$ is rational.
Proof: Suppose $(\sqrt{2})^{\sqrt{2}}$ is rational. Then we have an irrational that becomes rational when raised to the power $\sqrt{2}$.
Suppose now that $x = (\sqrt{2})^{\sqrt{2}}$ is irrational.
Then $x^{\sqrt{2}} = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\sqrt{2})} = (\sqrt{2})^2 = 2$, which is rational.

It is interesting that we can so easily conclude that either $\sqrt{2}$ or $(\sqrt{2})^{\sqrt{2}}$ is a candidate for the above theorem but deciding which one actually works requires a very deep mathematical argument. [In fact $x = (\sqrt{2})^{\sqrt{2}}$ is irrational (hard to prove) and $x^{\sqrt{2}}$ is rational (obvious).]

AND: $\mathbf{p \wedge q}$.
This is simply a case of two theorems rolled up into one.

$p \wedge q$
…….
Therefore p.
…….
Therefore q.
Hence $p \wedge q$.

Example 14: Prove that the sequence given by $u_n = 0$, $u_{n+1} = \sqrt{u_n + 3}$ converges as $n \to \infty$.

We use the theorem that increasing sequences, that are bounded above, converge.

So we must prove that $\forall n[u_{n+1} > u_n] \wedge \exists b\ \forall n[u_n < b]$. We prove each of these statements by induction on n.

$u_{n+1} > u_n$ for all n

We prove this by induction on n. $u_1 = \sqrt{3} > u_0 = 0$ so it holds for $n = 0$.

Suppose it is true for n, that is, $u_{n+1} > u_n$.

Then $u_{n+2}^2 - u_{n+1}^2 = u_{n+1} - u_n > 0$ so $u_{n+2}^2 > u_{n+1}^2$ and hence $u_{n+2} > u_{n+1}$.

(NB $u_n > 0$ for all n.)

Hence it is true for $n + 1$ and so, by induction, it is true for all n.

$u_n < 3$ for all n.

[Why 3? The reason is that when we calculate values of u_n we get the values:

0, 1.73205, 2.17533, 2.27493, 2.29672, ….

It appears that they will never exceed 3, so we try to prove that this guess is indeed correct. We do in fact succeed. But, had u_n eventually become bigger than 3, the proof would obviously break down. In that case we might have tried a larger number as a possible upper bound.]

We prove this by induction on n. $u_0 = 0 < 3$ so it holds for $n = 0$.

Suppose it is true for n, that is, $u_n < 3$.

Then $u_{n+1}^2 = u_n + 3 < 3 + 3 = 6$ so $u_{n+1} < \sqrt{6} < 3$.
Hence it is true for $n + 1$ and so, by induction, it's true for all n.

EQUIVALENCE: p ↔ q

This is essentially an "and" since p ↔ q is equivalent to $(p \to q) \wedge (q \to p)$.

p ↔ q	
Suppose *p*. …… Therefore *q*.	Now suppose *q*. …… Therefore *p*.
Hence $p \leftrightarrow q$.	

Example 15: Prove that if *p* is prime then it divides *mn* if and only if it divides *m* or *n*.

Solution: Suppose that *p* divides *m*. Then $m = pq$ for some integer *q* and so $mn = pqn$ and hence *p* divides *mn*. Similarly, if *p* divides *n*. (This is it the easy half of the proof.)

Now suppose that *p* divides *mn* and suppose *p* does not divide *m*.

(Here we need to prove '*p* divides *m* or *p* divides *n*' so we use the appropriate pattern of proof.)

So GCD(*p*, *m*) = 1.

Using a well-known fact about greatest common divisors we can write $1 = ph + mk$ for some integers *h, k*.

Hence $n = pnh + (mn)k$. Since *p* divides each of these terms, *p* divides *n*.

UNIVERSAL QUANTIFIER: $\forall x[Px]$

If we are to prove that something true for all x in S we begin by considering a typical x.

$\forall x[Px]$

Let $x \in$ S.

……

Therefore Px.

Hence $\forall x$[Px]

EXISTENTIAL QUANTIFIER: $\exists x[Px]$

When the proposition to be proved states that something exists with a certain property we need to define, or choose, a suitable x at some stage.

$\exists$**x[Px]**

Let $x = \ldots$

……

Therefore Px.

Hence $\exists x$[Px]

Often the x is not a particular x but rather something chosen with a certain property.

§1.13. The Importance of Definitions

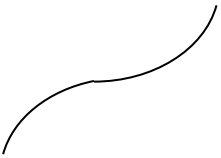
One of the major difficulties students have in writing proofs is not knowing how to handle definitions. The problem arises from the fact that a lecturer, when

presenting a new concept, generally begins by stating the formal definition. Because this will seem

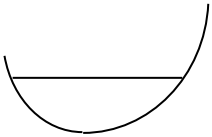
rather abstract to the student the lecturer then gives several informal versions and a number of illustrative examples. This is good and will improve the student's grasp of the concept. The problem is that all this illustrative stuff tends to overwrite the original formal definition in the student's mind. So when it comes to writing a proof based on that concept, the student encounters difficulty. It is important to remember that:

in writing proofs one should only use formal definitions

A 1-1 (one to one) function is one where different elements have different images or where you don't get a doubling up like you do when you square the numbers $-x$ and $+x$. If we can graph the function, it is 1-1 if you never have more than one part of the curve at any given level and not 1-1 if there are two or more parts at the same level. For example:



1-1



not 1-1

All this may very well help you to *understand* the concept but try to prove a theorem about 1-1 functions using the above collection of ideas!

The formal, technical, definition of the statement ***f* is 1-1** is the following:

if *f*(*x*) = *f*(*y*) then *x* = *y*.

Another problem often encountered is the difficulty of adapting a formal definition to the current circumstances and notation. It really is not such a difficult thing but you need to get into the right mind-set. Adapting a definition is simply a symbol substitution exercise. It doesn't require any intuitive understanding. It is simply an automatic and mindless operation with symbols, and in fact thinking about what the symbols mean only makes the exercise more difficult.
The definition of the 1-1 property can be recast as a rewriting rule:

whenever you encounter the string '□ **is 1-1**' you can replace it by

'if □(*x*) = □(*y*) then *x* = *y*'.

Here □ can stand for any symbol or collection of symbols that could represent a function.

So if you encounter '*g* is 1-1' you rewrite it as 'if $g(x) = g(y)$ then $x = y$'.

The statement '$g \circ f$ is 1-1' becomes 'if $g \circ f(x) = g \circ f(y)$ then $x = y$'. I will explain the meaning of the $\circ$ symbol later but the important thing to realise is that you don't need to understand the symbols in order to adapt a definition. It's simply a mindless clerical task with symbols. So '$\nabla \clubsuit +$ is 1-1' becomes:

'if $\nabla \clubsuit + (x) = \nabla \clubsuit + (y)$ then $x = y$'.

Now the statement 'if $f(x) = f(y)$ then $x = y$' contains a hidden quantifier. Strictly speaking it should read 'for all x and for all y, if $f(x) = f(y)$ then $x = y$', but we usually leave out the quantifiers in cases like this.

We can use any symbol we like for such dummy variables provided it does not have any other meaning. It would not be good to use "if $f(\pi) = f(2)$ then $\pi = 2$" to express the fact that f is 1-1 because the symbols π and 2 cannot be used as variables without some confusion. Also, if x has been used elsewhere, except as a dummy variable, then we can't use it here. So if the name of a function was T_x we couldn't write "if $T_x(x) = T_x(y)$ then $x = y$". We would need to replace the dummy variable x by something else, such as z and so write:
'if $T_x(z) = T_x(y)$ then $z = y$'.

But it *is* perfectly permissible to use x as a dummy variable several times provided the scope of the associated quantifiers don't overlap.

Another property of functions is the property of being 'onto'. Here we're thinking of functions not just as formulae, or rules to get $f(x)$ from x.

A function $f: S \to T$ is a pair of sets S, T together with a rule. The first set is called the **domain** of the function and the second set is called its **codomain**. A function is **onto** if every element of the codomain is the image of something in the domain. It is just like a target where every point on the target gets hit by an arrow. The function $f(x) = x^2$ is onto if the codomain is the set of real numbers x with $x \geq 0$ but is not onto if we consider f as a function to the set of *all* real numbers.

These analogies and example might help us to grasp the concept but to prove any theorem involving it we need to use the crisp, clear, but somewhat abstract-looking, formal definition.

The formal definition of a function being onto is:

$f: S \to T$ is onto if:
for all t in T there exists s in S such that $f(s) = t$,
or more briefly
$$\forall t \in T \; \exists s \in S \; [f(s) = t]$$

Here we're using the standard symbols for the quantifiers 'for all' and 'for some'. Also we're using the symbol '$\in$' to denote that something belongs to (or is an element of) some set. Finally the 'such that' serves no purpose except to make the sentence more readable, so we leave it out when writing the statement in symbols.

For the next example we need to know the definitions of 'onto' and '$\circ$', the composition of functions.
f:S $\rightarrow$ T is onto if for all t in T there exists s in S such that $f(s) = t$,
If f:A$\rightarrow$B and g:B$\rightarrow$C are functions then $g\circ f$:A$\rightarrow$C is the function $g\circ f(x) = g(f(x))$.

Example 16:
Let f:A$\rightarrow$B and g:B$\rightarrow$C be functions. Prove that if f is onto and $g\circ f$ is 1-1 then g is 1-1.
Proof:
(1) Suppose f is onto and $g\circ f$ is 1-1.
(We must write down our assumptions explicitly in the proof.)

(2) Suppose $g(b) = g(b')$.
(We write this because our goal is to prove that g is 1-1 and that says 'if g(b) = g(b′) then …')

(3) Since f is onto there exist a, $a' \in$ A such that $f(a) = b$ and f(a') = b'.
(We write this because the assumption that f is onto needs elements in B and we now have them.

(4) Hence $g(f(a)) = g(f(a'))$, that is $(g\circ f)(a) = (g\circ f)(a')$.
(We needed to get this so that we could use the assumption that $g\circ f$ is 1-1.

(5) Since $g\circ f$ is 1-1 we conclude that $a = a'$.

(But we are not quite finished.)

(6) Hence $f(a) = f(a')$, that is, $b = b'$.
(This is the conclusion to the statement that g is 1-1.)

(7) Therefore g is 1-1.

Here are some hints for writing proofs.

- Begin by writing down your assumptions.
- Examine the logical structure of the theorem and structure your proof accordingly.
- Keep asking yourself "what does that mean in more primitive terms?"
- Keep asking yourself "what is my current goal?" This changes throughout the proof.
- Use formal definitions.
- Work forward from what you know and back from what you have to prove, till they link up. But when you write the proof it must proceed in the direction from the assumptions to the goal.
- Never write down what you are trying to prove (unless you qualify it by such words as "we shall prove that …")
- Never prove that a statement holds for all x by merely considering one or more particular x's.

The following is a short list of formal definitions from various parts of mathematics written in the form of rewriting rules.

REWRITE …	AS …
n is even	there exists $m \in \mathbb{Z}$ such that $n = 2m$
$a \mid b$	$b = aq$ for some $q \in \mathbb{Z}$
p is a positive prime	$p > 1$, and if $p = ab$ for some $a, b \in \mathbb{Z}$ then $a = 1$ or $b = 1$
$f(x) \to \mathrm{L}$ as $x \to \infty$	for all $\varepsilon > 0$ there exists K such that if $\lvert x\rvert > \mathrm{K}$ then $\lvert f(x) - \mathrm{L}\rvert < \varepsilon$
$\mathrm{S} \subseteq \mathrm{T}$	if $s \in \mathrm{S}$ then $s \in \mathrm{T}$
$f{:}\mathrm{S} \to \mathrm{T}$ is 1-1	if $f(x) = f(y)$ then $x = y$
$f{:}\mathrm{S} \to \mathrm{T}$ is onto	If $t \in \mathrm{T}$ there exists $s \in \mathrm{S}$ such that $f(s) = t$
R is transitive	if $a\mathrm{R}b$ and $b\mathrm{R}c$ then $a\mathrm{R}c$
$\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ are linearly independent	if $\lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2 + \ldots + \lambda_n\mathbf{v}_n = \mathbf{0}$ then $\lambda_1 = \lambda_2 = \ldots = \lambda_n = 0$
$\mathrm{T}{:}\mathrm{U} \to \mathrm{V}$ is a linear transformation	For all $\mathbf{u}, \mathbf{u}' \in \mathrm{U}$: $\mathrm{T}(\mathbf{u} + \mathbf{u}') = \mathrm{T}(\mathbf{u}) + \mathrm{T}(\mathbf{u}')$ and $\mathrm{T}(\lambda\mathbf{u}) = \lambda\mathrm{T}(\mathbf{u})$ for all scalars λ

EXERCISES FOR CHAPTER 1

EXERCISES 1A (Truth Tables)

Ex 1A1: Use a Truth Table to prove that:

$$-q \vee (-p \rightarrow (p \leftrightarrow q)) \text{ is a tautology.}$$

Ex 1A2: Use a Truth Table to prove that:

$$(p \wedge -q) \rightarrow -(p \rightarrow q) \text{ is a tautology.}$$

Ex 1A3: Use a Truth Table to prove that:

$$(p \rightarrow (q \rightarrow r) \leftrightarrow -(p \wedge q) \vee r \text{ is a tautology.}$$

Ex 1A4: Use a Truth Table to determine whether or not the statement $p \wedge q \rightarrow -q \rightarrow p$ is a tautology.

Ex 1A5: Use a Truth Table to determine whether or not the statement $((p \rightarrow q) \rightarrow p) \rightarrow q$ is a tautology.

Ex 1A6: Use a Truth Table to show that the following statement is a tautology:

$$-[(p \leftrightarrow -q) \wedge (r \rightarrow p) \wedge (p \rightarrow q) \wedge r]$$

Ex 1A7: Use a Truth Table to prove that:

$$-(p \rightarrow q \wedge -r) \leftrightarrow (p \wedge (q \rightarrow r)$$

is a tautology.

Ex 1A8: Are $(p \rightarrow q) \rightarrow -p$ and $-(p \wedge q)$ equivalent?

Ex 1A9: Show that $(p \leftrightarrow -q) \wedge (r \rightarrow p)$ and $(p \rightarrow q) \wedge r$ are inconsistent.

Ex 1A10: Is the statement:

$$(r \rightarrow p \wedge q) \rightarrow ((r \vee s) \rightarrow (t \rightarrow p))$$

a tautology?

[**HINT:** A Truth Table for this question would have 64 rows which is a bit much. Instead, try to make the statement FALSE. You do this by making the first bit TRUE and the second bit FALSE. Continue in the same way.]

Ex 1A11: Prove that:

$$((q \vee r) \rightarrow (p \wedge s)) \rightarrow (s \rightarrow (p \rightarrow (q \vee r)))$$

is not a tautology.

Ex 1A12: Using Truth Tables, or otherwise, determine which of the following are tautologies.

(a) $(p \wedge q) \rightarrow (p \rightarrow q)$

(b) $-(p \rightarrow q) \leftrightarrow (-p \rightarrow -q)$

(c) $p \wedge -(q \wedge r) \leftrightarrow -(p \rightarrow q) \vee (p \wedge -r)$

(d) $((r \vee s) \rightarrow (p \wedge q)) \rightarrow (p \rightarrow (q \rightarrow (r \vee s)))$

Ex 1A13: Use a Truth Table to prove that:

$$-(p \rightarrow q) \vee (p \wedge q) \leftrightarrow p$$

is a tautology.

Ex 1A14: Use a Truth Table to prove this is a tautology:

$$(p \wedge q) \vee -(p \rightarrow q) \leftrightarrow p$$

EXERCISES 1B (Interpretation)

Ex 1B1: *If you're not staying on Great Keppel Island you're not having a perfect holiday.*
Express this in symbols. What does it say about the island?

Ex 1B2: Write out in symbols the sentence: 'exactly one of p, q and r is true'.

Ex 1B3: (a) Let Pxy denote the statement $xyx = x$. If the universe of quantification is the set of all real numbers, which of the following are TRUE?

(i) $\forall x \exists y$ Pxy;
(ii) $\exists x \forall y$ Pxy;
(iii) $\exists y \forall x$ Pxy ;
(iv) $\forall x \forall y$[P$xy \rightarrow$ Pyx];
(v) $\exists x$ Pxx.

(b) Repeat where the universe of quantification is the set of positive real numbers.
(c) Repeat when the universe of quantification is the set of positive integers.

Ex 1B4: Explain why the statement $x > y$ (for real numbers) can be written as

$$\forall z[-(y = x + zz)].$$

Ex 1B5: Express the following statement about real numbers symbolically, using only logical symbols and equations (no words or inequalities):

for all positive real numbers there is a smaller one

[**NOTE:** The only symbols you are allowed to use are the logical symbols, variables, brackets, '+' and '='. You may *not* use any other symbols such as $\mathbb{R}^+$ or inequalities. The Universe of Quantification is $\mathbb{R}$, which you don't have to mention explicitly.]

Ex 1B6: Express the statement '*m* and *n* have no common factor' in symbolic form using only logical symbols and primitive arithmetic statements of the form $x = yz$. (The universe of quantification is the set of positive integers.)

Ex 1B7: Which of the following are true? Give brief reasons.

(i) $\forall x \, \exists y \;\; [y < x]$ where the universe of quantification is $\mathbb{R}^+$ the set of all positive real numbers;

(ii) $\exists y \, \forall x \, [y < x]$ where the universe of quantification is $\mathbb{R}^+$, the set of all positive real numbers.

Ex 1B8: If the universe of quantification is $\mathbb{Z}$ the set of all integers, which of the following are true? Give brief reasons.

(i) $\forall x \, \exists y \;\; [x + y = 100]$;

(ii) $\exists y \, \forall x \, [x + y = 100]$;

(ii) $\forall x \, \exists y \;\; [xy + x^2 = 0]$;

(iv) $\exists y \, \forall x \, [x^2 y < x + 1]$.

EXERCISES 1C (Negation)

Ex 1C1: Negate the following statement:

$$\exists x[(x\mathrm{P}x \wedge -x\mathrm{Q}x) \wedge \forall y[x\mathrm{Q}y \wedge (-y\mathrm{P}y \wedge -y\mathrm{Q}x)]]$$

[This involves more than just writing the negation operator in front of it. You must apply the negation rules to put it the same form as the original statement, that is, where the negation operators are attached to the primitive statements.]

Ex 1C2: Negate the following statement:

$$\forall x[(x\mathrm{P}x \wedge -x\mathrm{Q}x) \rightarrow \exists y[-x\mathrm{Q}y \wedge (y\mathrm{P}y \wedge -y\mathrm{Q}x)]]$$

Ex 1C3: Negate the following statement, expressing the negation in its simplest form:

$$\forall x[\mathrm{P}x \rightarrow \exists y[x\mathrm{Q}y \vee -y\mathrm{Q}x]]$$

Ex 1C4: Negate the following statement, expressing the negation in its simplest form:

$$\exists x[x\mathrm{A}x \rightarrow \forall y[-x\mathrm{A}y \vee y\mathrm{A}x]]$$

Ex 1C5: Negate the following:

$$\forall x[\mathrm{P}x \rightarrow \exists y(\mathrm{Q}xy \wedge -\mathrm{P}y)].$$

Ex 1C6: Let P*nrk* denote the statement:

$$r < 1 \rightarrow 1 + r + r^2 + ... + r^n < k.$$

Which of the following are TRUE (give brief reasons). (The universe of quantification for r, k is the set of positive real numbers and the universe for n is the set of natural numbers.)

(i) $\forall r\ \exists k\ \forall n$ Pnrk; (ii) $\forall r\ \forall n\ \exists k$ Pnrk;
(iii) $\forall n\ \exists k\ \forall r$ Pnrk; (iv) $\exists k\ \forall r\ \forall n$ Pnrk
[**NOTE:** The same quantifiers are involved in each case, but the meaning changes when they are rearranged.]

Ex 1C7: Express the negation of:

$$\exists y[\mathrm{P}y \rightarrow \forall z[-\ y\mathrm{Q}z \wedge \mathrm{P}z]]$$

in such a way that the negation operator is only attached to primitive statements such as Px or xQy. Now write this in an equivalent, but simpler, form which doesn't use the negation operator at all.

EXERCISES 1D (Proof by Contradiction)

Ex 1D1:

(a) Translate the following theorem into symbolic form. [Use Ex for 'x is even' and Qx for 'x is quasimorphic' — never mind what that means]

Theorem: For all integers x there exists an integer y such that if x being even implies that y is not quasimorphic then x being quasimorphic implies that x is odd.

(b) Negate the above theorem (in symbolic form).
(c) Prove the theorem using Proof By Contradiction.
(d) Explain how you could prove a theorem without knowing what all the words mean?

Ex 1D2: Prove the following theorem:
Theorem: Either a database being quasiconsistent implies that it is implementable but incomplete or some database is either hyperclosed or quasiconsistent.

[**HINT:** This is a logical tautology (though because it involves quantifiers you cannot use truth tables). So you can prove it without knowing what the words 'database' 'quasiconsistent', "implementable", "incomplete", "hyperclosed" mean. Take as your universe the set of all databases. Let Ax = 'x is implementable'; Bx = 'x is quasi-consistent'; Cx = 'x is complete' and Dx = 'x is hyperclosed'. Express the statement symbolically and use Proof By Contradiction.]

Ex 1D3: Prove the following statement:
Theorem: Either a chromosome being bitractive implies that it is amphicheiral or discontinuous or there exists a chromosome which is bitractive but not amphicheiral.

EXERCISES 1E (Proofs involving 1-1 & Onto Functions

Ex 1E1: Let f:A$\rightarrow$B and g:B$\rightarrow$C be functions. Prove the following:
(a) if $g \circ f$ is 1-1 and f is onto then g is 1-1.
(b) if both f and g are onto then so is $g \circ f$.
(c) if both f and g are 1-1 then so is $g \circ f$.
(d) if $g \circ f$ is onto then so is g.

(e) if $g \circ f$ is onto and g is 1-1 then f is onto.

(f) if $g \circ f$ is 1-1 then so is f.

(g) (Harder) if $f \circ g \circ f$ is 1-1 and onto then so is g.

Ex 1E2: Let f:A$\rightarrow$A be a function where A is finite. Prove that f is 1-1 if and only if it is onto.

SOLUTIONS FOR CHAPTER 1

Ex 1A1: It is a tautology since it is TRUE in all cases.

–	q	∨	(–	p	→	(p	↔	q))
F	T	**T**	F	T	T	T	T	T
T	F	**T**	T	T	F	T	F	F
F	T	**T**	T	F	T	F	F	T
T	F	**T**	T	F	T	F	T	F

Ex 1A2: It is a tautology because it is TRUE in all cases.

p	∧	–	q)	→	–	(p	→	q)
T	F	F	T	**T**	F	T	T	T
T	T	T	F	**T**	T	T	F	F
F	F	F	T	**T**	F	F	T	T
F	F	T	F	**T**	F	F	T	F

Ex 1A3: It is a tautology since it is TRUE in all cases.

((p	→	(q	→	r))	↔	(–	(p	∧	q)	∨	r)
T	T	T	T	T	**T**	F	T	T	T	T	T
T	F	T	F	F	**T**	F	T	T	T	F	F
T	T	F	T	T	**T**	T	T	F	F	T	T
T	T	F	T	F	**T**	T	T	F	F	T	F
F	T	T	T	T	**T**	T	F	F	T	T	T
F	T	T	F	F	**T**	T	F	F	T	T	F
F	T	F	T	T	**T**	T	F	F	F	T	T
F	T	F	T	F	**T**	T	F	F	F	T	F

Ex 1A4: It is a tautology since it is TRUE in all cases.

(p	∧	q)	→	(–	q	→	p)
T	T	T	**T**	F	T	T	T
T	F	F	**T**	T	F	T	T
F	F	T	**T**	F	T	T	F
F	F	F	**T**	T	F	F	F

Ex 1A5: It is not a tautology since it is FALSE when p = T and q = F.

((p	→	q)	→	p)	→	q
T	T	T	T	T	T	T
T	F	F	T	T	**F**	F
F	T	T	F	F	T	T
F	T	F	F	F	T	F

Ex 1A6: It is a tautology since it is TRUE in all cases.

–	[((		↔	–	q	∧	(	→	p)	∧	((	→	q	∧	r)
	p				)		r		)		p		)		]
T	T	F	F	T	F	T	T	T	F	T	T	T	T	T
T	T	F	F	T	F	F	T	T	F	T	T	T	F	F
T	T	T	T	F	T	T	T	T	F	T	F	F	F	T
T	T	T	T	F	T	F	T	T	F	T	F	F	F	F
T	F	T	F	T	F	T	F	F	F	F	T	T	T	T
T	F	T	F	T	T	F	T	F	F	F	T	T	F	F
T	F	F	T	F	F	T	F	F	F	F	T	F	T	T
T	F	F	T	F	F	F	T	F	F	F	T	F	F	F

Ex 1A7: It is a tautology since it is TRUE in all cases.

–	(p	→	(q	∧	–	r))	↔	((p	∧	(q	→	r))
T	T	F	T	F	F	T	**T**	T	T	T	T	T
F	T	T	T	T	T	F	**T**	T	F	T	F	F
T	T	F	F	F	F	T	**T**	T	T	F	T	T
T	T	F	F	F	T	F	**T**	T	T	F	T	F
F	F	T	T	F	F	T	**T**	F	F	T	T	T
F	F	T	T	T	T	F	**T**	F	F	T	F	F
F	F	T	F	F	F	T	**T**	F	F	F	T	T
F	F	T	F	F	T	F	**T**	F	F	F	T	F

Ex 1A8: Statements S_1 and S_2 are equivalent if and only if $S_1 \leftrightarrow S_2$ is a tautology.
It is not, so they are not equivalent.

((p	→	q)	→	–	p)	↔	(–	(p	∧	q))
T	T	T	F	F	T	**T**	F	T	F	T
T	F	F	T	F	T	**F**	F	T	F	F
F	T	T	T	T	F	**T**	T	F	T	T
F	T	F	T	T	F	**T**	T	F	F	F

Ex 1A9: Statements S_1 and S_2 are inconsistent if and only if $-(S_1 \wedge S_2)$ is a tautology.
This was shown in Ex 1A6. So they are inconsistent.

Ex 1A10: Let us try to find a case which makes this FALSE without having to consider all 16 possibilities. We put F under the main → and work backwards.

(r	→	(p	∧	q))	→	((r	∨	s)	→	(t	→	p))
	T				**F**		T		F	T	F	F

So *t* = T and *p* = F. Now working forwards, as far as we can, we get:

(r	→	(p	∧	q))	→	((r	∨	s)	→	(t	→	p))
F	T	F	F		F		T		F	T	F	F

(Since p is FALSE, p ∧ q must be FALSE. But r → (p ∧ q) is TRUE, so r is FALSE.)
Transferring this across and continuing we get:

(r	→	(p	∧	q))	→	((r	∨	s)	→	(t	→	p))
F	T	F	F		F	F	T	T	F	T	F	F

So p = F, r = F, s = T and t = T. We can't deduce the truth value of q. All this means is that there are two cases which make the statement FALSE, one where q = T and one where it is FALSE. The fact that there is at least one case which makes the statement FALSE shows that it is not a tautology.

Ex 1A11: Let us try to home in on a case which makes this FALSE without having to consider all 16 possibilities. We put F under the main → and work backwards.

((q	∨	r)	→	(p	∧	s))	→	(s	→	(p	→	(q	∨	r))
			T				**F**	T	F	T	F	F	F	F

So p, s are TRUE and q, r are FALSE. Now working forwards we get:

((	∨	r	→	(	∧	s)	→	(	→	(	→	(	∨	r))
q		)		p		)		s		p		q		)
F	F	F	T	T	T	T	**F**	T	F	T	F	F	F	F

Since there is a consistent way of filling out this row of the table there is a case in which the statement is FALSE. Thus it is not a tautology.

Ex 1A12: (a) is a tautology.

(p	∧	q)	→	(p	→	q)
T	**T**	T	**T**	T	**T**	T
T	**F**	F	**T**	T	**F**	F
F	**F**	T	**T**	F	**T**	T
F	**F**	F	**T**	F	**T**	F

(b) is NOT a tautology.

–	(p	→	q)	↔	(–	p	→	–	q)
F	T	T	T	**F**	F	T	T	F	T
T	T	F	F	T	F	T	T	T	F
F	F	T	T	T	T	F	F	F	T
F	F	T	F	**F**	T	F	T	T	F

(c) is a tautology.

(p	∧	–	(q	∧	r))	↔	(–	(p	→	q)	∨	(p	∧	–	r))
T	**F**	F	T	T	T	**T**	F	T	T	T	**F**	T	F	F	T
T	**T**	T	T	F	F	**T**	F	T	T	T	**T**	T	T	T	F
T	**T**	T	F	F	T	**T**	T	T	F	F	**T**	T	F	F	T
T	**T**	T	F	F	F	**T**	T	T	F	F	**T**	T	T	T	F
F	**F**	F	T	T	T	**T**	F	F	T	T	**F**	F	F	F	T
F	**F**	T	T	F	F	**T**	F	F	T	T	**F**	F	F	T	F
F	**F**	T	F	F	T	**T**	F	F	T	F	**F**	F	F	F	T

F	**F**	T	F	F	F	**T**	F	F	T	F	**F**	F	F	T	F

(d) Let's try to find a case where it is FALSE.
If it is FALSE then $(r \vee s) \rightarrow (p \wedge q)$ is TRUE and
$p \rightarrow (q \rightarrow (r \vee s))$ is FALSE.
From the latter, p = T and $q \rightarrow (r \vee s)$ = F.
Thus q = T and $r \vee s$ = F.
Hence r, s are both FALSE.
So in the case p = T, q = T, r = F, s = F the statement is FALSE. Hence it is not a tautology.

Ex 1A13: is a tautology

[–	(p	→	q)	∨	(p	∧	q)]	↔	p
F	T	T	T	T	T	T	T	**T**	T
T	T	F	F	T	T	F	F	**T**	T
F	F	T	T	F	F	F	T	**T**	F
F	F	T	F	F	F	F	F	**T**	F

Ex 1A14: is a tautology

[(p	∧	q)	∨	–	(p	→	q)]	↔	p
T	T	T	T	F	T	T	T	**T**	T
T	F	F	T	T	T	F	F	**T**	T
F	F	T	F	F	F	T	T	**T**	F
F	F	F	F	F	F	T	F	**T**	F

Ex 1B1: Let g = "staying on Great Keppel Island" and let p = "having a perfect holiday".
The statement says that $-g \rightarrow -p$ which is equivalent to $p \rightarrow g$. It says you won't have a perfect holiday anywhere

else, but makes no claim about Great Keppel itself. Perhaps there's no such thing as a perfect holiday anywhere!

Ex 1B2: $(p \vee q \vee r) \wedge -(p \wedge q) \wedge -(p \wedge r) \wedge -(q \wedge r)$

Ex 1B3:
(a) (i) is TRUE. If $x \neq 0$, let $y = 1/x$. If $x = 0$, let $y =$ anything. Then $xyx = x$.
(ii) is TRUE. Take $x = 0$.
(iii) is FALSE. Putting $x = 1$ gives $y = 1$.
Putting $x = 2$ gives $y = ¼$.
So there is no such y.
(iv) is FALSE. Let $x = 0$ and $y = 1$. Then $xyx = x = 0$, but $yxy = 0 \neq y$.
(v) is TRUE. Let $x = 1$.

(b) (i) is TRUE. Let $y = 1/x$.
(ii) is FALSE, for taking $x = 1$ gives $y = 1$. But this would mean that $x^2 = x$ for all $x > 0$, which is not so.
(iii) is FALSE, as above.
(iv) is TRUE. If $xyx = x$ then $y = 1/x$ and $yxy = y$.
(v) is TRUE as above.

(c) (i) is FALSE. Take $x = 2$. The corresponding y would have to satisfy $4y = 2$, which has no solution in the positive integers.
(ii) is FALSE, as above.
(iii) is FALSE since (i) is FALSE.

(iv) is TRUE. If $xyx = x$ then $xy = 1$ and so $x = y = 1$ (only solution for positive integers). Thus $yxy = y$.
(v) is TRUE as above.

Ex 1B4: $(x > y) \leftrightarrow (y - x < 0)$. Negative real numbers are precisely those that have no square roots, so we can write this as:

$$x > y \leftrightarrow -\exists z\,[y - x = zz] \leftrightarrow \forall z[-(y - x = zz)]$$
$$\leftrightarrow \forall z[-(y = x + zz)].$$

Ex 1B5: The statement can be expressed as:

$$\forall x\,[x > 0 \rightarrow \exists y[(y > 0) \wedge (y < x)]].$$

Using Ex 1B3, we can write it in more primitive terms as:

$$\forall x\,[\forall z[-(x + zz = 0)]$$
$$\rightarrow \exists y[\forall z[-(y + zz = 0)] \wedge \forall z[-(y = x + zz)]].$$

Ex 1B6: The statement can be expressed as:

$$\forall d[((d \text{ divides } m) \wedge (d \text{ divides } n)) \rightarrow (d = 1)].$$

This can be expressed in more primitive terms as:

$$\forall d[\,(\exists q[m = dq] \wedge \exists q[n = dq]) \rightarrow (d = 1)]$$

NOTE: Since q is only a 'local variable' in each place we are able to use the same symbol each time, even though the q that works for m will generally be different to that which works for n.

Ex 1B7: (i) is TRUE. For example take $y = x/2$. (ii) is FALSE. If there was such a y, then taking $x = y$ we would get $y < y$ which is impossible.

Ex 1B8: (i) is TRUE. Take $y = 100 - x$;
(ii) is FALSE. If it was TRUE then all integers would be equal to $100 - y$;
(iii) is TRUE. Take $y = -x$;
(iv) is TRUE. Take $y = -1$.
Then $x^2y - x - 1 = -(x^2 + x + 1)$ which is always negative.

Ex 1C1: The negation is:

$$-\exists x[(x\mathrm{P}x \wedge -x\mathrm{Q}x) \wedge \forall y[x\mathrm{Q}y \wedge (-y\mathrm{P}y \wedge -y\mathrm{Q}x)]]$$
$$\leftrightarrow \forall x(-[(x\mathrm{P}x \wedge -x\mathrm{Q}x) \wedge \forall y[x\mathrm{Q}y \wedge (-y\mathrm{P}y \wedge -y\mathrm{Q}x)]])$$
$$\leftrightarrow \forall x(-(x\mathrm{P}x \wedge -x\mathrm{Q}x) \vee -\forall y[x\mathrm{Q}y \wedge (-y\mathrm{P}y \wedge -y\mathrm{Q}x)])$$
$$\leftrightarrow \forall x((-x\mathrm{P}x \vee -(-x\mathrm{Q}x)) \vee \exists y[-[x\mathrm{Q}y \wedge (-y\mathrm{P}y \wedge -y\mathrm{Q}x)]])$$
$$\leftrightarrow \forall x((-x\mathrm{P}x \vee x\mathrm{Q}x) \vee \exists y[(-x\mathrm{Q}y \vee -(-y\mathrm{P}y \wedge -y\mathrm{Q}x)]])$$
$$\leftrightarrow \forall x((-x\mathrm{P}x \vee x\mathrm{Q}x) \vee \exists y[(-x\mathrm{Q}y \vee (y\mathrm{P}y \vee y\mathrm{Q}x)]])$$

Ex 1C2: The negation is:

$$-\forall x[(x\mathrm{P}x \wedge -x\mathrm{Q}x) \rightarrow \exists y[-x\mathrm{Q}y \wedge (y\mathrm{P}y \wedge -y\mathrm{Q}x)]]$$
$$\leftrightarrow \exists x[-[(x\mathrm{P}x \wedge -x\mathrm{Q}x) \rightarrow \exists y[-x\mathrm{Q}y \wedge (y\mathrm{P}y \wedge -y\mathrm{Q}x)]]]$$
$$\leftrightarrow \exists x[(x\mathrm{P}x \wedge -x\mathrm{Q}x) \wedge -\exists y[-x\mathrm{Q}y \wedge (y\mathrm{P}y \wedge -y\mathrm{Q}x)]]$$
$$\leftrightarrow \exists x[(x\mathrm{P}x \wedge -x\mathrm{Q}x) \wedge \forall y[-[-x\mathrm{Q}y \wedge (y\mathrm{P}y \wedge -y\mathrm{Q}x)]]]$$
$$\leftrightarrow \exists x[(x\mathrm{P}x \wedge -x\mathrm{Q}x) \wedge \forall y[x\mathrm{Q}y \vee -(y\mathrm{P}y \wedge -y\mathrm{Q}x)]]$$
$$\leftrightarrow \exists x[(x\mathrm{P}x \wedge -x\mathrm{Q}x) \wedge \forall y[x\mathrm{Q}y \vee (-y\mathrm{P}y \vee y\mathrm{Q}x)]]$$

Ex 1C3: The negation is: $-\forall x[\mathrm{P}x \rightarrow \exists y[x\mathrm{Q}y \vee -y\mathrm{Q}x]]$

$$\leftrightarrow \exists x[-[\mathrm{P}x \rightarrow \exists y[x\mathrm{Q}y \vee -y\mathrm{Q}x]]]$$
$$\leftrightarrow \exists x[\mathrm{P}x \wedge -\exists y[x\mathrm{Q}y \vee -y\mathrm{Q}x]]$$
$$\leftrightarrow \exists x[\mathrm{P}x \wedge \forall y[-[x\mathrm{Q}y \vee -y\mathrm{Q}x]]]$$

$\leftrightarrow \exists x[\mathrm{P}x \wedge \forall y\,[-\,x\mathrm{Q}y \wedge y\mathrm{Q}x]]$

Ex 1C4: The negation is:
$-\exists x\,[x\mathrm{A}x \rightarrow \forall y[-\,x\mathrm{A}y \vee y\mathrm{A}x]]$
$\leftrightarrow \forall x\,-\,[x\mathrm{A}x \rightarrow \forall y[-\,x\mathrm{A}y \vee y\mathrm{A}x]]$
$\leftrightarrow \forall x\,[x\mathrm{A}x \wedge -\forall y[-\,x\mathrm{A}y \vee y\mathrm{A}x]]$
$\leftrightarrow \forall x\,[x\mathrm{A}x \wedge \exists y\,-\,[-\,x\mathrm{A}y \vee y\mathrm{A}x]]$
$\leftrightarrow \forall x\,[x\mathrm{A}x \wedge \exists \mathrm{y}\,[x\mathrm{A}y \wedge -\,y\mathrm{A}x]]$

Ex 1C5: The negation is: $-\forall x[\mathrm{P}x \rightarrow \exists y(\mathrm{Q}xy \wedge -\,\mathrm{P}y)]$
$\leftrightarrow \exists x\,-\,[\mathrm{P}x \rightarrow \exists y(\mathrm{Q}xy \wedge -\,\mathrm{P}y)]$
$\leftrightarrow \exists x\,[\mathrm{P}x \wedge -\exists y(\mathrm{Q}xy \wedge -\,\mathrm{P}y)]$
$\leftrightarrow \exists x\,[\mathrm{P}x \wedge \forall y\,-\,(\mathrm{Q}xy \wedge -\,\mathrm{P}y)]$
$\leftrightarrow \exists x[\mathrm{P}x \wedge \forall y(-\,\mathrm{Q}xy \vee \mathrm{P}y)]$.

Ex 1C6: (i) is TRUE, take k = sum to ∞;
(ii) is TRUE since $\exists k\,\forall n \rightarrow \forall n\,\exists k$;
(iii) is TRUE, take $k = n + 1$;
(iv) is FALSE, take $r = 1 - 1/(2k)$. Then $1/(1 - r) = 2k$. Since the sum to ∞ is $2k$ the sum of sufficiently many terms is greater than k.

1C7: $-\exists y[\mathrm{P}y \rightarrow \forall z[-\,y\mathrm{Q}z \wedge \mathrm{P}z]]$
$\leftrightarrow \forall y\,-\,[\mathrm{P}y \rightarrow \forall z[-\,y\mathrm{Q}z \wedge \mathrm{P}z]]$
$\leftrightarrow \forall y[\mathrm{P}y \wedge -\forall z[-\,y\mathrm{Q}z \wedge \mathrm{P}z]]$
$\leftrightarrow \forall y[\mathrm{P}y \wedge \exists z\,-\,[-\,y\mathrm{Q}z \wedge \mathrm{P}z]]$
$\leftrightarrow \forall y[\mathrm{P}y \wedge \exists z\,[y\mathrm{Q}z \vee -\,\mathrm{P}z]]$

$\leftrightarrow \forall y[Py \wedge \exists z\,[yQz]]$. This last step follows because if P*y* is TRUE for all y then in particular Pz is TRUE and so the $-$ Pz option is redundant.

Ex 1D1:

(a) $\forall x\, \exists y[(Ex \rightarrow - Qy) \rightarrow (Qx \rightarrow - Ex)]$.

(b) The negation is:

$- [\forall x\, \exists y[(Ex \rightarrow - Qy) \rightarrow (Qx \rightarrow - Ex)]]$

$\leftrightarrow \exists x\, -\exists y[(Ex \rightarrow - Qy) \rightarrow (Qx \rightarrow - Ex)]$

$\leftrightarrow \exists x\, \forall y - [(Ex \rightarrow - Qy) \rightarrow (Qx \rightarrow - Ex)]$

$\leftrightarrow \exists x\, \forall y\, [(Ex \rightarrow - Qy) \wedge - (Qx \rightarrow - Ex)]$

$\leftrightarrow \exists x\, \forall y\, [(Ex \rightarrow - Qy) \wedge (Qx \wedge Ex)]$.

(c) Suppose the theorem is FALSE.

Then $\exists x\, \forall y\, [(Ex \rightarrow - Qy) \wedge (Qx \wedge Ex)]$ which implies that in particular, taking $y = x$, that:

$$\exists x\, [(Ex \rightarrow - Qx) \wedge (Qx \wedge Ex)].$$

However $(Ex \rightarrow - Qx) \wedge (Qx \wedge Ex)$ can never be TRUE. So we obtain a contradiction by assuming that the theorem is FALSE. Hence it is TRUE.

(d) The 'theorem' actually has no actual content. It is true, simply because of its logical structure and would be TRUE no matter what the words 'quasimorphic' or 'even' meant.

Ex 1D2: (a) In symbols the statement becomes:
$\forall x[(Bx \rightarrow (Ax \wedge - Cx)] \vee \exists x[Dx \vee Bx]$
Suppose this is FALSE, ie suppose that:
$- [\forall x[(Bx \rightarrow (Ax \wedge - Cx)] \vee \exists x[Dx \vee Bx]]$. Then
$-\forall x[(Bx \rightarrow (Ax \wedge - Cx)] \wedge - \exists x[Dx \vee Bx]$.
$\therefore \exists x - [(Bx \rightarrow (Ax \wedge - Cx)] \wedge \forall x - [Dx \vee Bx]]$
$\therefore \exists x[(Bx \wedge - (Ax \wedge - Cx)] \wedge \forall x[- Dx \wedge - Bx]]$
$\therefore \exists x[(Bx \wedge (- Ax \vee - - Cx)] \wedge \forall x[- Dx \wedge - Bx]]$
$\therefore \exists x[(Bx \wedge (- Ax \vee Cx)] \wedge \forall x[- Dx \wedge - Bx]]$
Hence there is some x, for which Bx holds among other things. Yet for all x, Bx is FALSE (as well as Dx). Thus $\exists x\ Bx \wedge \forall x - Bx$, which is a contradiction.
Hence the theorem is true.

Ex 1D3: In symbols the statement is:
$\forall x[Bx \rightarrow (Ax \vee - Cx)] \vee \exists x[Bx \wedge - Ax]$.
Its negation is:
$- (\forall x[Bx \rightarrow (Ax \vee - Cx)] \vee \exists x[Bx \wedge - Ax])$
$\leftrightarrow -\forall x[Bx \rightarrow (Ax \vee - Cx)] \wedge -\exists x[Bx \wedge - Ax]$
$\leftrightarrow \exists x - [Bx \rightarrow (Ax \vee - Cx)] \wedge \forall x - [Bx \wedge - Ax]$
$\leftrightarrow \exists x[Bx \wedge - (Ax \vee - Cx)] \wedge \forall x[- Bx \vee Ax]$
$\leftrightarrow \exists x[Bx \wedge (- Ax \wedge Cx)] \wedge \forall x[- Bx \vee Ax]$.
It follows that $\exists x\ [Bx \wedge (- Ax \wedge Cx)]$.
Let k be such an x. Hence Bk and Ck are TRUE while Ak is FALSE.
But since $\forall x[- Bx \vee Ax]$ it follows that this holds for $x = k$.

Yet $-$ B$k \vee$ Ak is FALSE since Bk is TRUE and Ak is FALSE. Since the negation leads to a contradiction the original statement must be true.

Ex 1E1:

(a) Suppose $g(x) = g(y)$ for $x, y \in$ B. Since f is onto,
$x = f(u)$ for some $u \in$ A, and
$y = f(v)$ for some $v \in$ A. Thus $g(f(u)) = g(f(v))$, that is, $g \circ f(u) = g \circ f(v)$.
Since $g \circ f$ is 1-1 it follows that $u = v$. Hence $f(u) = f(v)$, that is, $x = y$.

(b) Suppose f is onto and g is onto. Let $c \in$ C. Since g is onto, $c = g(b)$ for some $b \in$ B. Since f is onto, $b = f(a)$ for some $a \in$ A. Then $c = g(b) = g(f(a)) = g \circ f(a)$.
Hence $g \circ f$ is onto.

(c) Suppose f and g are 1-1. Suppose that $g \circ f\,(x) = g \circ f$ (y). Then $g(f(x)) = g(f(y))$.
Since g is 1-1, $f(x) = f(y)$. Since f is 1-1, $x = y$.
Hence $g \circ f$ is 1-1.

(d) Suppose $g \circ f$ is onto. Let $z \in$ C.
Then $(g \circ f)(x) = z$ for some $z \in$ A.
Thus $g(f(x)) = z$. Hence g is onto.

(e) Suppose $g \circ f$ is onto and g is 1-1. Let $y \in B$. Then $g(y) \in C$. Hence, since $g \circ f$ is onto, $(g \circ f)(x) = g(y)$ for some $x \in A$. Thus $g(f(x)) = g(y)$. Since g is 1-1, $f(x) = y$. Thus f is onto.

(f) Suppose $g \circ f$ is 1-1 and that $f(x) = f(y)$.
Then $g(f(x)) = g(f(y))$, that is $(g \circ f)(x) = (g \circ f)(y)$.
Since $g \circ f$ is 1-1 it follows that $x = y$.

(g) Suppose $f \circ g \circ f$ is 1-1 and onto.
Suppose $g(x) = g(y)$ where $x, y \in B$.
Since $f \circ g \circ f$ is onto, there exist $x', y' \in A$ such that:
$x = (f \circ g \circ f)(x')$ and $y = (f \circ g \circ f)(y')$.
Hence $(f \circ g \circ f \circ g \circ f)(x') = (f \circ g \circ f \circ g \circ f)(y')$,
that is, $(f \circ g \circ f)(g(f(x'))) = (f \circ g \circ f)(g(f(y')))$.
Since $f \circ g \circ f$ is 1-1, $g(f(x')) = g(f(y'))$.
Thus $f(g(f(x))) = f(g(f(y)))$, that is, $f \circ g \circ f(x) = f \circ g \circ f(y)$.
Again, since $f \circ g \circ f$ is 1-1 we have $x' = y'$ and so $x = y$.

Suppose $x \in A$. Then $f(x) \in B$ and so $f(x) = (f \circ g \circ f)(y)$ for some $y \in A$.
Thus applying $f \circ g$ to both sides we get:

$$(f \circ g \circ f)(x) = (f \circ g \circ f \circ g \circ f)(y) = (f \circ g \circ f)(g(f(y))).$$

Since $f \circ g \circ f$ is 1-1 we have $x = g(f(y))$. Thus g is onto.

Ex 1E2: Suppose that A is finite and f:A$\rightarrow$A is 1-1. Then #f(A) = #A. A subset of a finite set that has the same number of elements as that set, must be the set itself, so f(A) = A and so f is onto.
Conversely suppose that f is onto. If $f(x) = f(y)$ for some $x \neq y$ then #f(A) < #A, contradicting the fact that f is onto.