R.P. McAfee

September 1986

ECONOMICS 241

HANDOUT

1.1 Boolean Logic

Mathematics is the study of various types of sentences. We are all familiar with sentences, but some examples won't hurt:

Example 1.1: Some sentences

Economists have no sense of humor. (1.1)

Women have fewer teeth than men. (1.2)

A blue moon gathers no moss. (1.3)

The aim of mathematics is to prove that some sentences are true, which essentially means that it is impossible for circumstances to arise that contradict the sentence. How might one go about proving the sentence with (1.1) to its right? Conceivably, one might construct a test for "sense of humor" and proceed to test all economists.

Indeed, the word "proof" originally meant "to test", as in "the proof of the pudding is in the eating". The problem with this is that, even if you establish that all living economists have no sense of humor, there is still a question of whether an economist could be born that had a sense of humor. Thus, one might hope to show that it is impossible for economists to have a sense of humor, i.e. that something in the definition of the term economist implies the utter lack of a funny bone. If you could somehow show this, you would have established that we never need to worry about a homorous economist ever appearing, its logically impossible.

This example captures the spirit of mathematics. We shall write down definitions of terms and show these logically imply other sentences are true. Before proving anything, we must establish some rules of reasoning, or laws of logic. That is, what are we allowed to conclude?

Some of the terms we shall use may be unfamiliar to the reader, so we summarize their meanings in Table 1.1 for future reference. We shall begin our inquiry into logic by considering very abstract sentences. Indeed, let A, B stand for sentences, any old sentences. We can construct new sentences from old ones with the following connectives:

<u>Connective</u>	<u>Meaning</u>	<u>Definition</u>
$\sim$	not	$\sim$A is true when A is false
$\vee$	or	A $\vee$ B is true when either A is true of B is true or both
$\wedge$	and	A $\wedge$ B is true when both A and B are true
$\Rightarrow$	implies	A $\Rightarrow$ B is true if, whenever A is true, B is true
$\Leftrightarrow$	if and only if	A implies B and B implies A

We take a sentence to be either true or false, that is, if the sentence A is not unconditionally true, then it is false. For example, "economists have no sense of humor" is false if there is a single economist with a sense of humor. However, the sentence "Most economists have no sense of humor" might be true if, say we define most to be more than 90%.

TABLE 1.1

Theorem: A sentence proved to be true.

Proposition: A sentence proved to be true.

Lemma: A Theorem which is used to prove another Theorem.

Corollary: A Theorem whose proof is obvious from the previous theorem.

Definition: A sentence taken to be true; one of the terms in the sentence is interpreted to make the sentence true.

Axiom, Assumption, Postulate: These are sentences taken to be true, alternatively, these sentences define the world we are considering.

Hypothesis: A sentence that will be checked for truth.

Tautology: A sentence which is true without assumptions, e.g. $x = x$.

Contradiction: A sentence that cannot be true, usually in the form "A is true and A is false"

The precise meaning of the 5 connectives can be given in a "truth table". Since only two initial sentences (A and B) were used, there are only 4 possible cases. Let T stand for "True" and F for "False".

A	B	~A	A∧B	A∨B	A⇒B	A⇔B
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

~~Case~~ row 1: Both A and B are true. This corresponds to row 1 in the truth table above. Note ~A is false (since A is true), A∧B is true (since both are true), A∨B is true (since at least one is true), A⇒B is true (since the hypothesis A is true and the implication B is as well), and A⇔B is true.

~~Case~~ row 2: A is true and B is false. This corresponds to row 2 in the truth table. ~A is false since A is true, A∧B is false since B is, A∨B is true since at least one (A) is true, A⇒B is false, since A is true and B isn't, thus A can't imply B.

We shall leave the remaining two rows to the reader, remarking only on A⇒B. When A is false, we take A⇒B to be true, since it is not contradicted. A⇒B is contradicted when A is true and B is false, and otherwise it is not contradicted. The effect is as if a monstrous bully asserted to you in a belligerant tone "A⇒B". Now you know full well that A is false, and so the implication A⇒B isn't very interesting. But you won't contradict him, either, since the assertion is not false, that is, its not contradicted. Effectively, A⇒B says "If A, then B. If not A, who knows?" and is true so long as we do not have ~A and B.

$\Leftrightarrow$, which may be read "if and only if" means $(A\Rightarrow B) \wedge (B\Rightarrow A)$, that is, when A is true, B is true, and vice versa. Thus A and B are either true together or false together when $A\Leftrightarrow B$. Thus, we can speak of $A\Leftrightarrow B$ as "A and B are equivalent". $\Leftrightarrow$ is also written iff or $\equiv$.

We are now in a position to prove some tautologies: sentences which are true no matter what A and B are.

Theorem 1.1: The following are tautologies

$$(\sim(\sim A))\Leftrightarrow A \qquad (1.4)$$

$$(\sim(A\wedge B))\Leftrightarrow((\sim A)\wedge(\sim B)) \qquad (1.5)$$

$$(\sim(A\vee B))\Leftrightarrow((\sim A)\vee(\sim B)) \qquad (.16)$$

$$(A\Rightarrow B)\Leftrightarrow((\sim A)\vee B) \qquad (1.7)$$

$$(A\Rightarrow B)\Leftrightarrow((\sim B)\Rightarrow(\sim A)) \qquad (1.8)$$

Proof: The only method we have available to prove these equivalences is the truth table, that is, we will explore all the possible cases. We start with (1.4).

A	~A	~(~A)	A ⇔ (~(~A))
T	F	T	T
F	T	F	T

Since, by definition, ~ reverses T for F and F for T, we obtain the second column. Reversing again yields the third column. Examining the first and third columns, we see (1.4) is true.

Now turn to (1.5)

A	B	~A	~B	(~A)V(~B)	A∧B	~(A∧B)
T	T	F	F	F	T	F
T	F	F	T	T	F	T
F	T	T	F	T	F	T
F	F	T	T	T	F	T

Again, the third column reverses the first, while the fourth reverses the second. $(\sim A)V(\sim B)$ becomes true if either $\sim A$ or $\sim B$ is true--all but the first row. The definition of $A \wedge B$ is given in column 6, and putting a not out front, $\sim(A \wedge B)$, reverses this for column 7. We then see that

$$((\sim A)\ V\ (\sim B)) \Leftrightarrow \sim(A \wedge B)$$

is true for all positions, and (1.5) is proved.

We can shorten the proof of (1.6) by using (1.4) and (1.5). Note (1.5) implies, for sentences C and D:

$$\sim(C \wedge D) \Leftrightarrow (\sim C)V(\sim D) \qquad (1.9)$$

Let $C = \sim A$, so $\sim C = \sim(\sim A) = A$ by (1.4)

Let $D = \sim B$, so $\sim D = \sim(\sim B) = B$ by (1.4).

Thus (1.9) is

$$\sim((\sim A) \wedge (\sim B)) \Leftrightarrow AVB \qquad (1.10)$$

Since, for any C, D,

$$(C \Leftrightarrow D) \Leftrightarrow ((\sim C) \Leftrightarrow (\sim D)) \qquad (1.11)$$

(1.10) becomes

$$\sim(AVB) \Leftrightarrow \sim\sim((\sim A) \wedge (\sim B)) \Leftrightarrow ((\sim A) \wedge (\sim B))$$

which proves (1.6). The reader should check (1.11) using a truth table.

We shall also leave (1.7) for the reader to prove, and turn to (1.8). Using (1.7) and

$$(AVB) \Leftrightarrow (BVA) \qquad (1.12)$$

(yet another obligation for the reader)

we have

$$(A\Rightarrow B) \overset{(1.7)}{\Leftrightarrow} ((\sim A)\vee B) \overset{(1.8)}{\Leftrightarrow} (B\vee(\sim A)) \overset{(1.4)}{\Leftrightarrow} ((\sim(\sim B))\vee(\sim A)) \overset{(1.7)}{\Leftrightarrow} (\sim B)\Rightarrow(\sim A)$$

Q.E.D.

'Q.E.D.' alerts the reader that the proof is over and its time to get on to other stuff. We shall state a few rules for the reader to prove:

$$(A\wedge B)\Leftrightarrow(B\wedge A) \qquad (1.13)$$

$$((A\wedge B)\wedge C)\Leftrightarrow(A\wedge(B\wedge C)) \qquad (1.14)$$

$$((A\vee B)\vee C)\Leftrightarrow(A\vee(B\vee C)) \qquad (1.15)$$

$$(A\wedge(B\wedge C))\Leftrightarrow((A\wedge B)\vee(A\wedge C)) \qquad (1.16)$$

$$(A\vee(B\wedge C))\Leftrightarrow((A\vee B)\wedge(A\vee C)) \qquad (1.17)$$

(1.12) and (1.13) are called commutativity. (1.14) and (1.15) are the associative laws, or associativity, and finally (1.16) and (1.17) represent distributativity.

There are several other tautologies of use.

$$(A\wedge(A\Rightarrow B))\Rightarrow B \qquad (1.18)$$

$$((\sim A)\Rightarrow(B\wedge(\sim B)))\Rightarrow A \qquad (1.19)$$

(1.18), called "modus ponens" or the syllogism, states that, from A and $A\Rightarrow B$, we may deduce B. This is the rule of logic (proveable given our definitions of $\wedge$ and $\Rightarrow$) that forms the basis of logical reasoning. Verbally, "if A is true and A implies B, then B is true."

Statements of the form $B\wedge(\sim B)$ are always false; $B\wedge(\sim B)$ is called a contradiction. (1.19) says that, if ~A leads to a contradiction, then A is true. That is, one way to prove A is to hypothesize ~A, and show that this leads to a contradiction.

(1.8) is called the contrapositive, and says that A implies B is the same as "whenever B is false, A is false." This is intuitively reasonable (as are all tautologies, if you think about them enough), since A implies B means that, to not get B being true, A must have been false.

This is about as far as "Boolean Logic", the logic of connectives (connectives being things like and, or , not, implies, and if and only if) can take us. However, we now have 16 tautologies (1.4-1.~~0~~19) that we can apply in our reasoning to come.

We end this section by noting the boolean logic has an arithmetic. Let T be 1 and F be zero, so if A is true, it takes on the numerical value 1, and otherwise it is 0. Then

$$\sim A = 1-A$$

$$A \wedge B = \min\{A,B\}$$

$$A \vee B = \max\{A,B\}$$

$$A \Rightarrow B = \max\{1-A, B\}$$

where min{A,B} is the smaller of A,B and max{A,B} is the larger.

<u>Quantifiers</u>

Quantifiers will establish the number or quantity of things x having some property A(x). For example, let x range over economists, A(x) mean "x has a sense of humor". Then (1.1) asserts "for all x, A(x)". We abbreviate "for all x" by

$$(\forall x)A(x) \text{ means for all } x,\ A(x) \text{ is true.} \qquad (1.20)$$

Thus, we have allowed our sentences to have a variable in them, something that can take on any value in a universe or domain of discourse. In the example above, the universe was the collection of economists. Generally, we shall denote our universe by U. A(x) is then a property of things in U, and x either has the property (and A(x) is true) or doesn't (and then A(x) is false).

Economists are generally interested in questions of existence. For example, does there exist a market clearing price? Is there an economist with a sense of humor? When there is an x with the property A(x), we write

$$(\exists x)A(x) \text{ means for some } x \text{ in } U,\ A(x) \text{ is true} \qquad (1.21)$$

We may observe immediately that

$$\sim((\exists x)A(x))\Leftrightarrow(\forall x)(\sim A(x)) \qquad (1.22)$$

$$\sim((\forall x)A(x))\Leftrightarrow(\exists x)(\sim A(x)) \qquad (1.23)$$

(1.22) says, in words, if it is not true that there is an x satisfying A(x), then all x satisfy ~A(x), and vice versa. Similarly, (1.23) says, if it is not true that A(x) is true for all x, then there must exist a counter example, an x satisfying ~A(x), and vice versa.

From (1.22) and (1.23), the reader may easily verify

$$(\forall x)A(x)\Leftrightarrow\sim(\exists x)(\sim A(x)) \qquad (1.24)$$

$$(\exists x)A(x)\Leftrightarrow\sim(\forall x)(\sim A(x)) \qquad (1.25)$$

In addition

$$(\exists x)(A(x) \vee B(x)) \Leftrightarrow ((\exists x)A(x) \vee (\exists x)B(x)) \qquad (1.26)$$

$$(\forall x)(A(x) \wedge B(x)) \Leftrightarrow ((\forall x)A(x) \wedge (\forall x)B(x)) \qquad (1.27)$$

$$(\exists x)(A(x) \wedge B(x)) \Rightarrow (\exists x)A(x) \wedge (\exists x)B(x) \qquad (1.28)$$

$$((\forall x)A(x) \vee (\forall x)B(x)) \Rightarrow (\forall x)(A(x) \vee B(x)) \qquad (1.29)$$

(1.26) shows that, if there is an x satisfying $A(x) \vee B(x)$, then either there is an x satisfying $A(x)$ or there is an x satisfaying $B(x)$, and vice versa. The point is that the same x works on either side.

Similarly, if $A(x) \wedge B(x)$ is true for every x then $(\forall x)A(x)$ and $(\forall x)B(x)$. However, if $(\forall x)A(x)$ and $(\forall x)B(x)$, clearly $A(x) \wedge B(x)$ is true for every x.

The attractive symmetry we have discovered so far (in section 1, replacing ands with ors and ors with ands left expressions (involving $\wedge$, $\vee$ and ~ [redacted]) unchanged breaks down with quantifiers, as we see from (1.28) and (1.29), which are not expressed as if and only if. To give an example of (1.28), suppose x ranges over economists (U is the collection of economists). $A(x)$ means x is over six feet tall and $B(x)$ means x is under six feet. Then it may well be true that $(\exists x)A(x) \wedge (\exists x)B(x)$, i.e. there is one economist over six feet tall and another under six feet tall, but clearly there cannot be any economist satisfying $(\exists x)(A(x) \wedge B(x))$, since this would make him both over and under six feet tall. One other quantifier of use is "there exists a unique x", and we write

$$(\exists ! x)A(x)$$

to mean there is one, and only one, x in U satisfying $A(x)$. Notationally

$$(\exists ! x)A(x) \Leftrightarrow ((\exists x)A(x)) \wedge (\forall y)(\forall z)((A(y) \wedge A(z)) \Rightarrow y = z).$$

Verbally, if there is a unique x, there is at least one satisfying $A(x)$, and if y, z are any two satisfying A, (i.e. $A(y) \wedge A(z)$) they y and z are the same.

Always, in the background, the universe U determines the x's we are talking about. Sometimes it will be useful to make this explicit, that is, to remind ourselves x must be in U and we write

$$x \in U$$

to mean "x is a member of U" or x is in the collection U. If U is the collection of shoes, then $x \in U$ is true when x is a shoe, and otherwise false.

The reader should be cautioned that $(\forall x)(\exists y)A(x,y)$ is not the same as $(\exists y)(\forall x)A(x,y)$. Let, by way of example, $A(x,y)$ be the statement $y=x^2$. Then, for every x, there is a number y satisfying $y=x^2$. However, there is no y which makes the statement $(\forall x)y=x^2$ true, for this would imply x^2 is the same no matter what x is, which is clearly false. Indeed, the reader may verify that

$$(\exists y)(\forall x)A(x,y) \Rightarrow (\forall x)(\exists y)A(x,y)$$

but not vice versa.

1.3 Sets

Sometimes we may be interested in portions of the universe. Suppose U is the collection of shoes, and let B(x) mean x is blue. Then the collection, or set, of blue shoes is denoted

$$\{x \in U/B(x)\}$$

or just

$$\{x/B(x)\} \qquad (1.30)$$

where the universe is understood in (1.30). (1.30) should be read "the set of x such that B of x is true". One interesting set is the empty set, a set that has no members:

$$\phi = \{x/A(x) \land \sim A(x)\} \qquad (1.31)$$

The empty set ϕ serves the same role in the theory of sets as 0 serves in the counting numbers; it is a placeholder.

Definition 1.1:

$$\{x/A(x)\} \cup \{x/B(x)\} = \{x/A(x) \vee B(x)\} \quad (1.32)$$

$$\{x/A(x)\} \cap \{x/B(x)\} = \{x/A(x) \wedge B(x)\} \quad (1.33)$$

$$\{x/A(x)\}^c = \{x/{\sim}A(x)\} \quad (1.34)$$

This defines three notions from elementary school mathematics, that of union ($\cup$), intersection ($\cap$), and complement (^{c}) in terms of logical connectives ($\vee$, $\wedge$ and $\sim$). (1.32) says that something gets into the union by being in one or the other set, gets into the intersection by being in both, and gets in the complement by not being in the set. Since we have identified sets by sentences which characterize them, it is natural to call

$$\{x/A(x)\} = A$$

By definition, $x \in A$ if $A(x)$ is true. Note that we are using A both for the set and the sentence defining the set, but this ambiguity in the meaning of the letter A causes no problem, since the set is defined by the sentence.

Theorem 1.2:

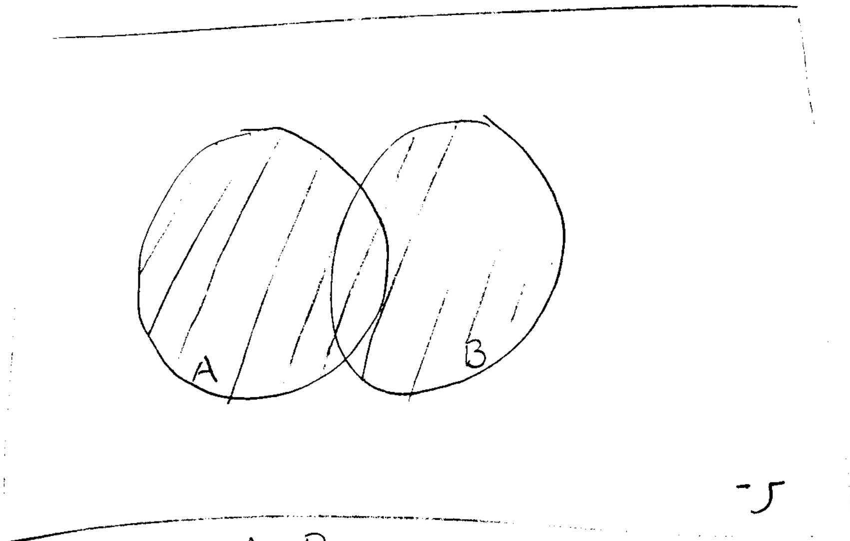
$$x \in A \cup B \Leftrightarrow ((x \in A) \vee (x \in B)) \quad (1.35)$$

$$x \in A \cap B \Leftrightarrow ((x \in A) \wedge (x \in B)) \quad (1.36)$$

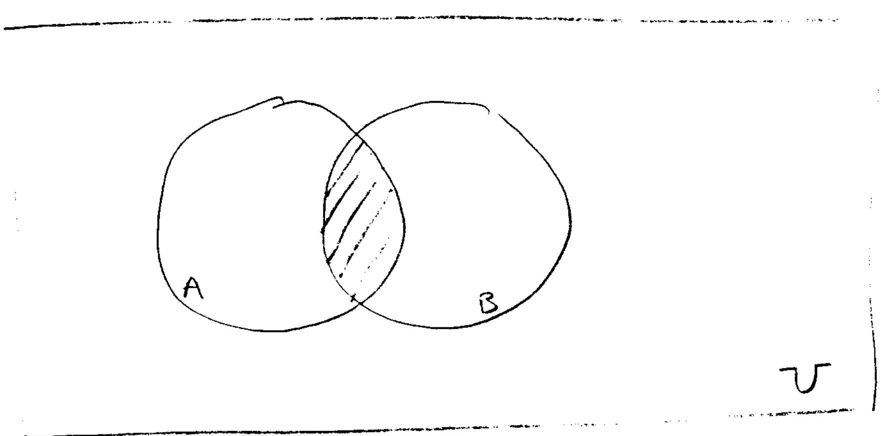
$$x \in A^c \Leftrightarrow {\sim}(x \in A) \quad (1.37)$$

Proof: $x \in A \cup B \overset{(1.32)}{\Leftrightarrow} A(x) \vee B(x) \Leftrightarrow (x \in A) \vee (x \in B)$. Others are similar.

Theorem 1.2 is illustrated by the Venn diagrams in figure 1.1. The universe U is the points inside the rectangle. The set A is the points inside the circle marked A, and the set B is the points inside the circle marked B. $A \cup B$, $A \cap B$ and A^c are illustrated. When ${\sim}(x \in A)$, we will write $x \notin A$.



A ∪ B



A ∩ B

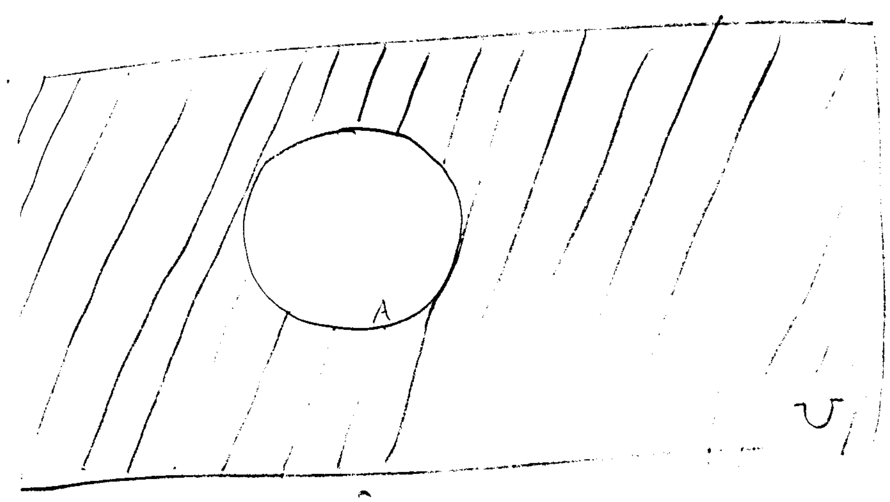


Figure 1.1

Theorem 1.3:

$$A \cap A^c = \phi \tag{1.38}$$

$$A \cup A^c = \mathcal{U} \tag{1.39}$$

$$\{x/A(x) \Rightarrow B(x)\} = A^c \cup B \tag{1.40}$$

Proof: To show two sets are the same, we show that they have the same elements.

$$x \in A \cap A^c \overset{(1.36)}{\Leftrightarrow} (x \in A) \wedge (x \in A^c) \overset{(1.34)}{\Leftrightarrow} A(x) \wedge \sim A(x) \overset{(1.31)}{\Leftrightarrow} x \in \phi .$$

$x \in A \cup A^c \Leftrightarrow (x \in A) \vee (x \in A^c) \Leftrightarrow$

$A(x) \vee \sim A(x) \Leftrightarrow x \in \{x/A(x) \vee \sim A(x)\}$.

Since $A(x) \vee \sim A(x)$ is a tautology,

$x \in A \cup A^c \Leftrightarrow x \in \mathcal{U}$.

(1.40) follows from (1.7) Q.E.D.

Theorem 1.4 (De Morgan's Laws):

$$(A \cup B)^c = A^c \cap B^c \tag{1.41}$$

$$(A \cap B)^c = A^c \cup B^c \tag{1.42}$$

De Morgan's laws are the set theory version of (1.5) and (1.6), and the proof follows directly from these facts.

Intersection and union are not limited to finitely many operations, but to generalize this, we need the notion of an index set. Let Γ be a set of names of sets, so that, if $i \in \Gamma$, A_i is a set. For example, Γ might be all the names of the states, and A_i, for state i, might be the names of people living in state i. Alternatively, Γ might be a list of album titles, and A_i the set of people who own album i. Thus, for this example, the intersection of A_i for all $i \in \Gamma$ would be those people who own all the albums on the list, since a person gets into A_i by owning album i, they must own all the albums to get into the intersection. To get into the union of the A_i's, you must get into at least one of the A_i's, and thus you must own at least one record. Consequently, the union of the A_i's is the set of people who own at least one record~~s~~ (in the list Γ).

For the intersection of the A_i's, $i \in \Gamma$, we write $\bigcap_{i\in\Gamma} A_i$, and for union we write $\bigcup_{i\in\Gamma} A_i$. The discussion suggests the following definition:

Definition 1.2:

$$\bigcup_{i\in\Gamma} A_i = \{x/(\exists i\in\Gamma)(x\in A_i)\} \tag{1.43}$$

$$\bigcap_{i\in\Gamma} A_i = \{x/(\forall i\in\Gamma)(x\in A_i)\} \tag{1.44}$$

Theorem 1.5 (De Morgan's Laws):

$$\left(\bigcup_{i\in\Gamma} A_i\right)^c = \bigcap_{i\in\Gamma} A_i^c \tag{1.45}$$

$$\left(\bigcap_{i\in\Gamma} A_i\right)^c = \bigcup_{i\in\Gamma} A_i^c \tag{1.46}$$

Proof: We prove (1.45) and leave (1.46) to the reader. To prove (1.45), we shall show

$$x \in \left(\bigcup_{i\in\Gamma} A_i\right)^c \Leftrightarrow x \in \bigcap_{i\in\Gamma} A_i^c$$

This forces the sets to have the same elements, and hence be the same set.

$$x \in \left(\bigcup_{i\in\Gamma} A_i\right)^c \overset{(1.37)}{\Leftrightarrow} \sim\left(x \in \bigcup_{i\in\Gamma} A_i\right) \overset{(1.43)}{\Leftrightarrow}$$

$$\sim((\exists i\in\Gamma)(x \in A_i)) \overset{(1.22)}{\Leftrightarrow} (\forall i\in\Gamma)(\sim(x\in A_i)) \overset{(1.37)}{\Leftrightarrow}$$

$$(\forall i\in\Gamma)(x\in A_i^c) \overset{(1.44)}{\Leftrightarrow} x\in \bigcap_{i\in\Gamma} A_i^c.$$ Q.E.D.

Previously, we have identified sets with statements A(x), and showed the relationship between connectives $\wedge$, $\vee$ and ~, and set operations $\cap$, $\cup$ and complement. Definition 1.2 shows that role that quantifiers play in set theory: they allow big unions and intersections, since the set Γ may have infinitely many elements.

Definition 1.3: $A \subseteq B$ (read A is contained in B) if $x\in A\Rightarrow x\in B$. In this case, we say A is a subset of B.

Theorem 1.6: Let $A = \{x/A(x)\}$, $B = \{x/B(x)\}$.

Then $A \subseteq B$ if and only if $(\forall x)(A(x)\Rightarrow B(x))$.

Proof: $A \subseteq B \Leftrightarrow x\in A \Rightarrow x\in B \Leftrightarrow A(x) \Rightarrow B(x)$. Q.E.D.

Finally, we note that

$$A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A \Leftrightarrow (\forall x)A(x)\Leftrightarrow B(x). \quad (1.47)$$

This completes the development of the relationship of logical connectives and set theory, since we have seen that the connectives ~, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$ correspond to the set theory notions complement, intersection, union, containment, and equality.

We conclude this section with a celebrated paradox invented by Bertrand Russell.

Theorem 1.7 (Russell's paradox): The collection of all sets is not a set.

Proof: We shall show that presuming that the collection of all sets is a set leads to a contradiction, which, by (1.19),allows us to conclude the theorem.

Suppose the set of all sets is a set. Call if V. Then we may define the subset A of V by

$$A = \{x \in V/x \notin x\} \quad (1.48)$$

where $x \notin x$ means $\sim(x \in x)$. A is a set, so we may ask: is A an element of A? By the definition of A,

$$A \in A \Leftrightarrow \sim(A \in A) \qquad (1.49)$$

by substituting A for x in (1.48). (1.49) is in the form $B \Leftrightarrow \sim B$, and this is a contradiction since, if B is true, $B \Rightarrow \sim B$ yields $B \wedge \sim B$. On the other hand, if $\sim B$ is true, $\sim B$ and $\sim B \Rightarrow B$ implies $(\sim B) \wedge B$. Either way, we have a contradiction.

Q.E.D.

Russell's paradox caused quite a brouhaha in mathematics, because mathematicians were used to calling any old collection of things, including collections of sets, a set. The problem with this arises when a set is defined in terms of itself, as in (1.48). Since A is a set, $A \in V$, and thus we are defining A in terms of itself--one of the elements used to construct A is A itself. This self-reflexive construction permits contradictions to arise in a manner exactly analogous to the problem of the sentence:

This sentence is false. (1.50)

If (1.50) is true, it is false, and if its false, its true. Thus (1.50) leads to a paradox because it refers to itself, in a sense, before it is already constructed. Thus, it refers to something that is not yet defined, the sentence itself. The solution to this paradox is to restrict our attention to constructs that have been defined, and thus build up new constructs from old ones, being careful to never define a construct in terms of itself. This turns out to be an unnecessarily severe restriction (since it turns out that there are some meaningful sentences that do imply things about the sentence itself), but the distinction will not be useful for this text.

Functions

Sometimes we shall refer to a set X as a space, and this means nothing beyond X is a set.

Definition 1.4: Let X, Y be sets. The cross product (or cartesian product) of X and Y, denoted X x Y is the set of ordered pairs

$$X \times Y = \{(x,y) / x \in X \wedge y \in Y\}.$$

Example 1.2: Let X = {a,b,c} and Y = {d,e}.

Then

X x Y = {(a,d), (a,e), (b,d), (b,e), (c,d), (c,e)}.

Example 1.3: The plane. Let X = Y = R be the (real) number line. Then R x R (which we will call R^2) is the plane. See figure (1.2).

We can repeatedly apply Definition 1.4 to build up ordered triples, ordered quadruples and so forth. Generally

$$X_1 \times X_2 \times \ldots \times X_n = \{(x_1, x_2, \ldots, x_n) / x_1 \in X_1 \wedge x_2 \in X_2 \wedge \ldots \wedge x_n \in X_n\} \qquad (1.51)$$

and $(x_1, x_2, \ldots, x_n)$ is called a tuple, n-tuple or vector.

We use the following shorthand

$$\mathop{\mathrm{X}}_{i=1}^{n} X_i = X_1 \times X_2 \times \ldots \times X_n \qquad (1.52)$$

$$X^n = \mathop{\mathrm{X}}_{i=1}^{n} X \qquad (1.53)$$

Example 1.4: Suppose X is the set of characters on a typewriter keyboard (including the space, period, etc.). Then X^2 is the set of things of two characters in length that can be typed. Generally, X^n is the set of things of n characters that can be typed.

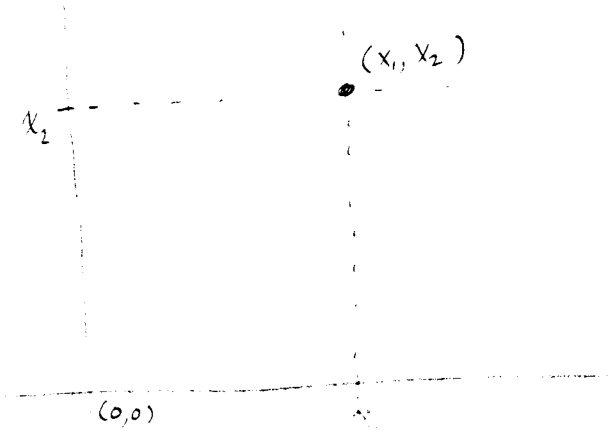


figure 1.2 $(x_1, x_2) \in R^2$

Example 1.5: Suppose there are n goods, numbered 1, 2, 3,...,n. Let a person's consumption of good i be x_i. If $x_i < 0$, the person has negative consumption, that is, he supplies the good. Thus $(x_1, x_2, \ldots x_n)$ represents one person's consumption, and the space of such n tuples is the set of possible consumption bundles. This space is known as R^n.

Definition 1.5: A function F from X to Y, denoted $F:X \to Y$, is a subset $F \subseteq X \times Y$ satisfying

$$(\forall x \in X)(\exists y \in Y)\ (x,y) \in F \tag{1.54}$$

$$((x,y) \in F \wedge (x,z) \in F) \Rightarrow y=z \tag{1.55}$$

F is 1-1 ("one to one") if

$$((x,y) \in F \wedge (z,y) \in F) \Rightarrow x = z \tag{1.56}$$

F is onto if

$$(\forall y \in Y)(\exists x \in X)\ (x,y) \in F \tag{1.57}$$

From (1.54) and (1.55), a function associates a single element of Y with each element of X. This allows the more familiar version of writing functions

$$y = f(x) \Leftrightarrow (x,f(x)) \in F \tag{1.58}$$

As figure 1.3 illustrates, a function defines a graph. Figure 1.4 illustrates a graph that is not a function. Generally, we'll call the range of f

$$\text{range of } f = \{y \in Y / (\exists x \in X)\ y = f(x)\} \tag{1.59}$$

Theorem 1.8

$$\text{range of } f = Y \Leftrightarrow f \text{ is onto} \tag{1.60}$$

There is a function g: $Y \to X$ satisfying:

$g(f(x)) = x \wedge f(g(y)) = y$ if and only if f is 1-1 and onto.

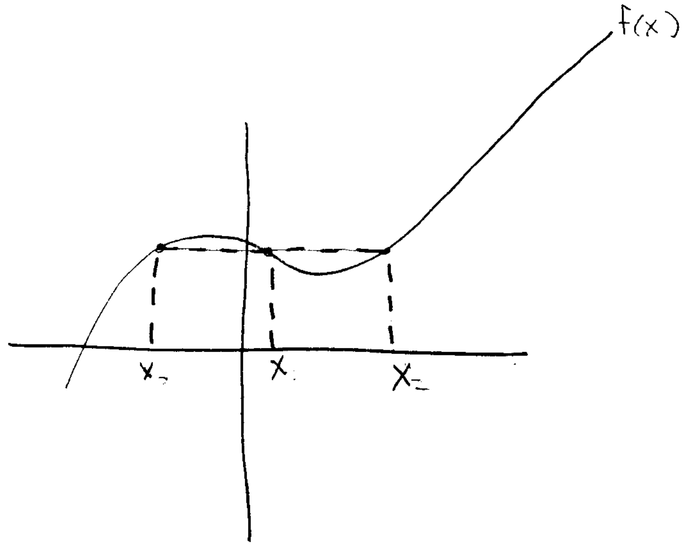


Figure 1.3: A function in the plane. f is not 1-1 since x_0, x_1 and x_2 are all associated with the same value y.

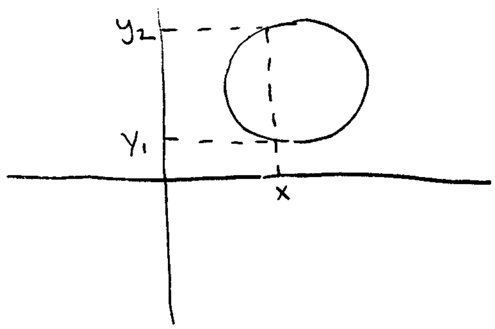


Figure 1.4: The graph of a circle is not a function, since two values of Y are associated with a single x, violating 1.55.

Proof: (1.60) is left as an exercise. To prove the second assertion, we use two parts.

(Proof of $\Rightarrow$): Suppose g(f(x)) = x and g is a function.

For any y, note x = g(y) satisfies

$$f(x) = f(g(y)) = y$$

Thus $(\forall y \in Y)\ (\exists x \in X)\ f(x) = y$

proving f is onto.

In addition, since g is a function if f(x) = f(z), we have

$$x = g(f(x)) = g(f(z)) = z,$$ so f is 1-1.

(Proof of $\Leftarrow$): Suppose F is 1-1 and onto.

Define G: $Y \to X$ by $(y,x) \in G \Leftrightarrow (x,y) \in F$.

Since F is onto

$$(\forall y \in Y)\ (\exists x \in X)\ (x,y) \in F, \text{ or}$$

$$(\forall y \in Y)\ (\exists x \in X)\ (y,x) \in G.$$

Thus G satisfies (1.54).

Since F is 1-1

$$((x,y) \in F \wedge (z,y) \in F) \Rightarrow x=z$$

or

$$((y,x) \in G \wedge (y,z) \in G) \Rightarrow x=z.$$

Thus G satisfies (1.55).

Finally

$$(x,f(x)) \in F \Rightarrow (f(x), x) \in G \Rightarrow x = g(f(x)).$$

Let y = f(x). Then

$$y = f(x) = f(g(f(x)) = f(g(y))$$

since x = g(f(x)). Q.E.D.

The function g of Theorem 1.8 is said to be f's inverse, or f^{-1}, because it cancels f:

$$f(f^{-1}(x)) = f^{-1}(f(x)) = x \tag{1.61}$$

1.5 Odds and Ends

In this section, we shall remind the readers of some properties of numbers, introduce some notation, and discuss some conventions that will persist throughout the text.

The natural numbers are the counting numbers:

$$N = \{0, 1, 2, 3, \ldots\} \tag{1.62}$$

The integers are the natural numbers plus negative natural numbers

$$Z = \{\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\} \tag{1.63}$$

The rational numbers Q are fractions

$$Q = \{m/n \,/\, m \in Z \wedge n \in N \wedge n \neq 0\} \tag{1.64}$$

The rationals (for "ratio") are fractions like 2/3, $-5/2 = -2\tfrac{1}{2}$, $3.141 = \frac{3141}{1000}$, and so forth.

We will primarily be concerned with the "real numbers", R. A careful definition will be provided in the next chapter, but, for the moment, think of the real numbers as a line, and each point on the line corresponds to a real number.

Absolute value is defined by

$$|x| = \sqrt{x^2} = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases} \tag{1.65}$$

Square roots are always taken to be nonnegative. The second part of the definition comes in two parts, and is understood to mean

$$(x \geq 0 \Rightarrow |x| = x) \wedge (x < 0 \Rightarrow |x| = -x).$$

Square roots are defined by

$$\sqrt{x} = y \Leftrightarrow (y \geq 0 \wedge y^2 = x) \qquad (1.66)$$

where y^2 is merely y times y. Absolute value has the important property

$$|x + y| \leq |x| + |y| \qquad (1.67)$$

since

$$2xy \leq 2|xy| = 2|x||y|$$

or

$$x^2 + 2xy + y^2 \leq x^2 + 2|x||y| + y^2 = |x|^2 + 2|x||y| + |y|^2$$

or

$$(x + y)^2 \leq (|x| + |y|)^2$$

or

$$|x + y| \leq |x| + |y|.$$

In addition, for real numbers λ and x:

$$|\lambda x| = |\lambda||x|. \qquad (1.68)$$

The real numbers have a property called the archimedian property:

$$(\forall x \in R)(\exists n \in N)\ |x| < n \qquad (1.69)$$

Thus, if $\varepsilon > 0$, there is a natural number n with $1/\varepsilon < n$, or $\varepsilon > 1/n$. That is

$$(\forall \varepsilon > 0)(\exists n \in N)(1/n < \varepsilon) \qquad (1.70)$$

One notational convenience is summation notation. Suppose x_i is a number for each i in an index set Γ. Then

$$\sum_{i \in \Gamma} x_i$$

represents the sum of all the x_i's, $i \in \Gamma$. For example, if $\Gamma = \{1,2,3\}$

$$\sum_{i \in \Gamma} x_i = x_1 + x_2 + x_3$$

when $\Gamma = \{1,2,3,\ldots,n\}$, it is conventional to write

$$\sum_{i=1}^{n} x_i = x_1 + x_2 + x_3 + \ldots + x_n \qquad (1.71)$$

The reader unfamiliar with summation notation may wish to convert into (1.71) notation, and prove the following

$$\sum_{i \in \Gamma_1} \sum_{j \in \Gamma_2} x_{(i,j)} = \sum_{j \in \Gamma_2} \sum_{i \in \Gamma_1} x_{(i,j)} = \sum_{v \in \Gamma_1 \chi \Gamma_2} x_v \qquad (1.72)$$

$$\left(\sum_{i=1}^{n} x_i\right)\left(\sum_{j=1}^{m} y_j\right) = \sum_{i=1}^{n} x_i \left(\sum_{j=1}^{n} y_j\right) = \sum_{i=1}^{n} \sum_{j=1}^{n} x_i y_j \qquad (1.73)$$

A special case of (1.73) is

$$(x_1 + x_2)(y_1 + y_2) = x_1(y_1 + y_2) + x_2(y_1 + y_2)$$
$$= x_1y_1 + x_1y_2 + x_2y_1 + x_2y_2 \qquad (1.74)$$

If λ is a constant:

$$\lambda\left(\sum_{i=1}^{n} x_i\right) = \sum_{i=1}^{n} \lambda x_i \qquad (1.75)$$

The reader may have already noticed that important lines of the text are numbered sequentially as 1.n. We will continue this, where the number before the decimal point indicates the chapter, and the number after the equation. Theorems and definitions will be numbered in a similar fashion. Thus, we may refer to Theorem 2.11 (the eleventh theorem of chapter 2), Definition 3.2 (the second defintion of chapter 3), or (4.21), which is the 21st numbered line in chapter 4.

Throughout the text, unless otherwise stated, α, β, γ, λ and θ will refer to real numbers. q will be a rational. i, j, k, m and n will be integers or natural numbers. x, y, and z will be members of the set being studied (e.g. real numbers in chapter 2, vectors in chapter 3, members of R^n in chapter 4, etc.). This convention will be continued with subscripts (e.g. α_j, β_i are reals, q_i is a rational).

1.6 A Taxonomy of Proofs

This chapter has developed a large number of rules of logic, that is, methods of manipulating connectives and quantifiers. All of our proofs will involve these rules, but in addition to this, there are several broad categories proofs generally fall into, and we shall discuss these here.

First, there is the direct proof. Typically, a direct proof will be used for a theorem in the form $A \Rightarrow B$. The strategy, then, is to find intermediate "steps" so $A \Rightarrow A_1$ and $A_1 \Rightarrow A_2$ and $A_2 \Rightarrow A_3, \ldots$ are all tautologies, and there is a final $A_n = B$. Thus, notationally, the direct proof is a sequence $A \Rightarrow A_1 \Rightarrow A_2 \Rightarrow \ldots \Rightarrow A_{n-2} \Rightarrow A_{n-1} \Rightarrow B$. Another description would be as a list

A

A_1

A_2

.

.

.

A_{n-2}

A_{n-1}

B

where each intermediate step A_i is either a tautology or follows from the previous steps, i.e.

$$(A \wedge A_1 \wedge \ldots A_{i-1}) \Rightarrow A_i$$

is a tautology.

Typically, such a strategy requires a very large number of steps, so often we will collapse the steps, which, strictly speaking, leaves a piece of the job for the reader to do (to insert the remaining steps). However, we shall indicate what is used in filling in the missing pieces. For example, if we write

$$A_i \overset{(1.19)}{\Rightarrow} A_{i+1}$$

This means that the tautology proved in (1.19) makes the step from A_i to A_{i+1}.

Direct proofs may involve cases, that is, it may be simpler to perform the proof in pieces. For example, if we wish to prove

$(\forall x)\ (A(x) \Rightarrow x=0)$

It may be easier to prove

case 1: $(\forall x)\ (A(x) \Rightarrow x \geq 0)$

and

case 2: $(\forall x)\ (A(x) \Rightarrow x \leq 0)$.

Then, using

$(x \geq y \wedge x \leq y) \Rightarrow x = y$

we have proved $(\forall x)(A(x) \Rightarrow x=0)$.

In some situations, to prove a statement in the form $A \Rightarrow B$, it may be convenient to split A into cases. That is, show $A \Leftrightarrow (A_1 \vee A_2)$ and then show $A_1 \Rightarrow$ ~~B~~ A and $A_2 \Rightarrow$ ~~B~~ A. For example, to prove

$(0 \leq x \leq 1) \Rightarrow x^2 \leq x$

we write

$(0 \leq x \leq 1) \Leftrightarrow (x=0 \vee (0 < x \leq 1))$

and do the case, first $x=0$ and then $0 < x \leq 1$, as in the latter case, we may divide by x.

One other aspect of direct proofs bears mention. If the theorem comes in the form $A \Leftrightarrow B$, it is generally easier to prove two separate theorems: $A \Rightarrow B$ and $B \Rightarrow A$. In such an instance, these two parts will be denoted by ($\Rightarrow$) and ($\Leftarrow$) (the second for $A \Leftarrow B$).

A useful tool for proving theorems in the form $A \Rightarrow B$ is the contrapositive (1.18). To prove $A \Rightarrow B$, it is sufficient to prove $(\sim B) \Rightarrow (\sim A)$ instead. These proofs will begin by "Proof: By contrapositive."

Yet another attack on theorems is the proof by contradiction. Generally, to prove A, we may instead show

$$\sim A \Rightarrow (B \wedge \sim B)$$

which, by (1.19), proves A. $B \wedge \sim B$ is the contradiction. For instance, we may show $x \geq 0$ and $x < 0$, but since $\sim(x \geq 0) \Leftrightarrow x < 0$, we have a contradiction. In particular, for theorems in the form $A \Rightarrow B$, since

$$\sim(A \Rightarrow B) \Leftrightarrow A \wedge (\sim B)$$

we shall show $A \wedge (\sim B)$ leads to a contradiction, which proves $A \Rightarrow B$.

One other proof technique works for the natural numbers only, and is called induction. Suppose we wish to show

$$(\forall n \in \mathbb{N})\ A(n)$$

is true.

We shall instead prove

$$A(0) \wedge (\forall n \in \mathbb{N})(A(n) \Rightarrow A(n+1))$$

This works because $A(0)$ is true, and $A(0) \Rightarrow A(1)$ yields $A(1)$. $A(1) \Rightarrow A(2)$ then yields $A(2)$. $A(2) \Rightarrow A(3)$ yields $A(3)$, and so on.

A more formal description of why induction works can be given, if the well-ordering property of the natural numbers is used

Axiom (well ordering): $(\forall A \subseteq N)(A \neq \phi \Rightarrow (\exists a \in A)(\forall b \in A)(a \leq b))$

In words: Any nonempty subset of N has a least element. Thus, if $(\forall n \in N)\ A(n)$ fails to be true, then.

$$(\exists n \in N)(\sim A(n))$$

Thus

$$\{n \in N / \sim A(n)\}$$

has a least element. Call it K. Either K=0, and

$$\sim A(0)$$

or $K > 0$, in which case we have

$$(\sim A(K)) \wedge A(K-1)$$

since K is the least number satisfying $\sim A(K)$, and hence $A(K-1)$ is true. But

$$\sim A(0) \vee (A(K-1) \wedge \sim A(K)) \overset{n=K-1}{\Leftrightarrow}$$

$$\sim A(0) \vee (\exists n \in N)(A(n) \wedge (\sim A(n+1))) \Leftrightarrow$$

$$\sim (A(0) \wedge (\forall n \in N) \sim (A(n) \wedge (\sim A(n+1)))) \Leftrightarrow$$

$$\sim (A(0) \wedge (\forall n \in N)(A(n) \Rightarrow A(n+1))).$$

That is, if $(\forall n \in N)\ A(n)$ fails to be true, then $A(0) \wedge (\forall n \in N)(A(n) \Rightarrow A(n+1))$ fails to be true. By the contrapositive:

$A(0) \wedge (\forall n \in N)(A(n) \Rightarrow A(n+1))$ implies $(\forall n \in N)\ A(n)$.

Example 1.6

We show $(\forall n \in N) \sum_{i=0}^{n} \lambda^{i} = \frac{1-\lambda^{n+1}}{1-\lambda}$ if $\lambda \neq 1$. (1.76)

The property A(n) is $\sum_{i=o}^{n} \lambda^{i} = \frac{1-\lambda^{n+1}}{1-\lambda}$.

A(0) is true, since

$$\sum_{i=o}^{o} \lambda^{i} = \lambda^{o} = 1$$

and

$$\frac{1-\lambda^{o+1}}{1-\lambda} = \frac{1-\lambda}{1-\lambda} = 1.$$

We now show

$$A(n) \Rightarrow A(n+1).$$

That is, given

$$\sum_{i=0}^{n} \lambda^{i} = \frac{1-\lambda^{n+1}}{1-\lambda} \tag{1.77}$$

we show

$$\sum_{i=0}^{n+1} \lambda^{i} = \frac{1-\lambda^{(n+1)+1}}{1-\lambda} = \frac{1-\lambda^{n+2}}{1-\lambda} .$$

But by the definition of summation notation

$$\sum_{i=0}^{n+1} \lambda^{i} = \sum_{i=0}^{n} \lambda^{i} + \lambda^{n+1}$$

$$= \frac{1-\lambda^{n+1}}{1-\lambda} + \lambda^{n+1} \qquad \text{(by 1.77)}$$

$$= \frac{1-\lambda^{n+1}+(1-\lambda)\lambda^{n+1}}{1-\lambda} \qquad \text{(common denominator)}$$

$$= \frac{1-\lambda^{n+1}+\lambda^{n+1}-\lambda^{n+2}}{1-\lambda}$$

$$= \frac{1-\lambda^{n+2}}{1-\lambda}, \text{ as desired.}$$

The following provides a good test of the reader's understanding of induction:

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2} \tag{1.78}$$

$$\sum_{i=0}^{n} i(i+1) = \frac{n(n+1)(n+2)}{3} \tag{1.79}$$

$$\sum_{i=0}^{n} i(i+1)(i+2)\ldots(i+K) = \frac{n(n+1)(n+2)\ldots(n+K)(n+K+1)}{K+2} \tag{1.80}$$

(this requires induction over n and K!).

$$\sum_{i=0}^{n} \frac{1}{(i+1)(i+2)} = \frac{n+1}{n+2} \tag{1.81}$$

For $j \leq n$; $\lambda \neq 1$:

$$\sum_{i=j}^{n} \lambda^{i} = \frac{\lambda^{j}-\lambda^{n+1}}{1-\lambda} \tag{1.82}$$

For $\lambda \neq 1$:

$$\sum_{i=0}^{n} i\lambda^{i} = \frac{\lambda-(n+1)\lambda^{n+1}+n\lambda^{n+2}}{(1-\lambda)^{2}} \tag{1.83}$$

The general discussion in this section provides the 5 major types of proofs: direct, by cases, by contrapositive, by contradiction and by induction. We shall see many examples of each, and will note at the beginning of the proof if contrapositve, contradiction or induction is used.