Foundations of mathematics
Summer 2013

D.D Kodwani

May 9, 2014

Beginning date: August 31, 2013
Instructor: Dr Rajesh Thakkar

Abstract

Physics and almost all of science is written in the language of mathematics. So it is important to learn the foundations of mathematics to be able to succeed as a physicist. In fact some parts of theoretical physics are just branches of mathematics, a prime example is string theory which does not have many testable predictions but is a mathematical framework. Geometry is required to understand general relativity and aspects of linear algebra are necessary for quantum field theories. On the application side of things, Fourier analysis is a major tool for almost everything; from signal processing, electronics to astronomy.

Contents

1 Logic **3**

1.1 Statement . . . 3
1.2 Connectives . . . 4
1.3 Truth values & tables . . . 4
1.4 De Morgan's Laws: Equivalent statements . . . 8
1.5 Conditional statements . . . 10
1.6 Bi-conditional statements . . . 12
1.7 Tautology and contradiction . . . 14
1.8 Algebra of statements . . . 17
1.8.1 Commutative law . . . 17
1.8.2 Associative law . . . 17
1.8.3 Identity law . . . 18
1.8.4 Complement law . . . 19
1.8.5 Distributive law . . . 19
1.8.6 Idempotent law . . . 20
1.8.7 De Morgan's laws . . . 20
1.8.8 Contrapositive law . . . 20
1.8.9 Law of double negation . . . 21
1.8.10 Transitive law . . . 21
1.8.11 Law of addition . . . 21
1.8.12 Law of simplification . . . 22
1.9 Deductive reasoning . . . 22
1.10 Argument . . . 23
1.11 Joint denial . . . 26
1.12 Inverting truth tables . . . 28
1.13 Application: Circuits . . . 30

2 Set Theory **41**

2.1 Sets . . . 41
2.2 Equality of sets . . . 42
2.3 Subsets . . . 42
2.4 Null set . . . 43
2.5 Power set . . . 49
2.6 Operation with sets . . . 51
2.6.1 Union . . . 51
2.6.2 Intersection . . . 55
2.6.3 Complements . . . 60
2.7 Algebra of sets . . . 63
2.7.1 Law of Idempotence . . . 63
2.7.2 Commutative laws . . . 63
2.7.3 Associative law . . . 63
2.7.4 Distributive laws . . . 63
2.7.5 De-Morgans laws . . . 64
2.8 VENN Diagrams . . . 66
2.9 Applications . . . 69
2.10 Cartesian product of two sets . . . 80
2.11 Relation . . . 83
2.11.1 Representation of a relation by a matrix . . . 85

2.11.2 Diagrammatical representation of a relation 86
2.12 Mapping 86
2.12.1 One-One mapping 88
2.12.2 Onto mapping 88
2.12.3 Binary composition 90
2.13 Boolean Algebra 90
2.13.1 Example of Boolean algebras 97

3 Groups, Rings and Fields 99
3.1 Introduction to Groups 99
3.2 Properties 104
3.2.1 Identity element in a group, G, is unique 104
3.2.2 Cancellation law 104
3.2.3 Inverse of each $a \in G$ is unique 104
3.2.4 Inverse of an inverse, $(a^{-1})^{-1} = a$ 105
3.2.5 Associativity of inverse, $(ab)^{-1} = b^{-1}a^{-1}$ 105
3.3 Power elements of groups 120
3.4 Rings 122
3.5 Commutative ring 123
3.6 Ring with unity 123
3.6.1 Properties 128
3.7 Integral Domain 131
3.8 Fields 132
3.8.1 Equality between fields and integral domain 135

1 Logic

Logic is one of these words that is used in everyday life, but with an ambiguity about its true meaning. Of course the word might carry different meanings depending on which context it is being used in. The underlying meaning of logic is the analysis of language (not be confused with semantics) and its study involves the learning of the principles and methods employed in distinguishing valid arguments from those that are not valid.

This definition of logic will cover almost any context in which the word is being used. There are always questions about what logic really is and how it should be interpreted, but being mathematicians (or physicists), let us not worry about that. Let's start the analysis of logic by defining the most fundamental part of logic, which is a *statement.*

1.1 Statement

In our everyday language we come across statement that may be interrogative or declarative/exclamatory.

- **Interrogative**: A sentence that demands a response. The most common example is a question:
  What is your name?
  This is an interrogative statement.

- **Declarative**: A sentence that states a fact, opinion or intention. An example might be:
  I am the best.

In mathematics, however, a declarative sentence which is either true or false is called a *statement.* An example of a true statement:
There is no real number, x, such that $x^2 = 1$

An example of a false statement:
The sun is square in shape

On the other hand:
Do you know what time it is?

Is not a statement, but:
The time is 4.50 pm
Is a statement.

All of these statements fall into the category of being *simple statement.* A statement which is made up of two or more simple statements is called a *compound* statement. An example is:
The sum of three angle in a triangle in Euclidean geometry two right angles and the sum of the lengths of two sides of a triangle is greater then the length of the

third side.

Now one might get a feel for what logic and statements really are. In fact they will probably sound familiar to computer scientists. A computer is built upon logic and the concept of true and false statements (this is how logic gates are built). These underlying concepts have a very deep meaning and lie at the foundations of information theory. For example, a simple statement will generally convey a single piece of information which we might call one *bit* of information. Compound statements will generally carry more than one bit of information. One thought about it carefully, information theory lied at the heart of all of physics. Just like energy and momentum are always conserved in nature, so is information. This is the basis behind deterministic laws. In the study of logic, letters from the English alphabet are usually used to represent statement.

1.2 Connectives

There are many ways of combining statements to form a compound statement. The words which combine simple statements to form compound statements are called connectives. There are five connectives which are used frequently. These are:

- *and*: denoted by $\wedge$ (also called conjunction)
- *or*: denoted by $\vee$ (also called dis-conjunction)
- *not*: denoted by $\sim$ (also called negation)
- *implies*: denoted by $\Rightarrow$
- *if and only if*: denoted by $\Leftrightarrow$

The connectives $\wedge$ and $\vee$ may be placed between any two statements to form compound statements. For example, if d and k are two statements then we can form compound statements like:

$$d \wedge k \tag{1.2.1}$$

$$d \vee k \tag{1.2.2}$$

The compound statement $d \wedge k$ is true if and only if both d and k are true. So, if d is false or k is false or both d and k are false, then $d \vee k$ is true and conversely too. The statement $\sim$ is false when p is true and it is true when p is false.

1.3 Truth values & tables

If a statement is true, we say its truth is T and if it is false we say it has a truth value of F.

A table that gives truth values of a compound statement is called a *Truth table*. In the initial columns, we write the possible truth values of the constituent statements and in the last column the truth value of the compound statement is written (which, of course, depends upon the values written in the initial columns). If a compound statement is made up of two simple statements then the number of rows will be 2^2 and if its made up of three statements then the number of rows will be 2^3 and so in general the number of rows is:

$$\text{no of rows} = 2^n \tag{1.3.1}$$

where n is the number of statements in a compound statements. These are best understood in terms of examples:

Example 1

Problem: Let d be a statement. Construct the truth table for $\sim d$.

Solution: We know that $\sim d$ is true when d is false and $\sim d$ is false when d is true. So the truth table is:

d	$\sim d$
T	F
F	T

Table 1: Truth table for $\sim d$

Example 2

Problem: Let d and k be two statements. Construct the truth table for the compound statement $d \wedge k$.

Solution: We know that $d \wedge k$ is true if and only if d and k are both true. The truth table is:

d	k	d $\wedge k$
T	T	T
T	F	F
F	T	F
F	F	F

Table 2: Truth table for $d \wedge k$

Example 3

Problem: Construct the truth table for the compound statement $d \vee k$

Solution: We know that $d \vee k$ is false if and only if d is false and k is false. Therefore the truth table is:

d	k	d $\vee k$
T	T	T
T	F	T
F	T	T
F	F	F

Table 3: Truth table for $d \wedge k$

Example 4

Problem: Construct the truth table for $\sim((\sim d) \wedge (\sim k))$

Solution: This is a compound statement which is much more complicated, however we can just follow the same logic and find the truth table:

d	k	$\sim d$	$\sim k$	$(\sim d) \wedge (\sim k)$	$\sim((\sim d) \wedge (\sim k))$
T	T	F	F	F	T
T	F	F	T	F	T
F	T	T	F	F	T
F	F	T	T	T	F

Table 4: Truth table for $\sim((\sim d) \wedge (\sim k))$

Example 5

Problem: Construct the truth table for $(d \wedge k) \wedge \sim d$

Solution: The truth table is:
So we see that this compound statement is always false.

d	k	d $\wedge k$	$\sim d$	$(d \wedge k) \wedge \sim d$
T	T	T	F	F
T	F	F	F	F
F	T	F	T	F
F	F	F	T	F

Table 5: Truth table for $(d \wedge k) \wedge \sim d$

Example 6

Problem: Construct the truth table for $\sim ((\sim d) \vee (\sim k))$

Solution: The truth table is:

d	k	$\sim d$	$\sim k$	$\sim d \vee \sim k$	$\sim ((\sim d) \vee (\sim k))$
T	T	F	F	F	T
T	F	F	T	T	F
F	T	T	F	T	F
F	F	T	T	T	F

Table 6: Truth table for $\sim ((\sim d) \vee (\sim k))$

Example 7

Problem: Lets define the following statements;

d = The south-west monsoon is very good this year

k = Rivers are rising

Give the verbal statements for:

$$d \vee \sim k \qquad (1.3.2)$$

$$\sim (\sim d \vee \sim k) \qquad (1.3.3)$$

Solution: Lets start with $d \vee \sim k$. $\sim k$ means the rivers are not rising, therefore $d \vee \sim k$ stands for "'The south-west monsoon is very good this year or the rivers are not rising"'.

Now lets discuss $\sim (\sim d \vee \sim k)$. $\sim d$ stands for "'The south-west monsoon is not very good this year. $\sim k$ means the rivers are not rising. Therefore the compound statement says that the south-west monsoon is not very good this year and neither are the rivers rising."'

1.4 De Morgan's Laws: Equivalent statements

Two statements d and k are said to be equivalent if they have the same truth values for *all* logical possibilities. If two statements are required we write:

$$d \equiv k \tag{1.4.1}$$

In other words, two statements are equivalent if they have the same truth tables. For example, the truth tables of $d\ k$ and $\sim(\sim d \wedge \sim k)$ are the same (look at the truth tables of the previous examples), implying that:

$$d\ \vee k \equiv \sim(\sim d \wedge \sim k) \tag{1.4.2}$$

Example 8

Problem: Prove the following statements:

$$\sim(d\ \vee k) \equiv \sim d \wedge \sim k \tag{1.4.3}$$

$$\sim(d\ \wedge k) \equiv \sim d \vee \sim k \tag{1.4.4}$$

Solution: The only way to prove these is by writing down the truth tables. First lets do Eq 1.4.3:

d	k	d $\vee k$	$\sim(d\ \vee k)$	$\sim d$	$\sim k$	$\sim d \wedge \sim k$
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

Table 7: Truth table for $\sim(d\ \vee k) \equiv \sim d \wedge \sim k$

This is the combined truth table and since column 4 and 7 are the same the relation is true.

Now lets do Eq 1.4.4:

d	k	d $\wedge k$	$\sim (d\ \wedge k)$	$\sim d$	$\sim k$	$\sim d \vee \sim k$
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

Table 8: Truth table for $\sim (d\ \vee k) \equiv \sim d \wedge \sim k$

These relations in Eq 1.4.3 and Eq 1.4.4 are collectively known as De Morgan's laws.

Example 9

Problem 1: Prove $\sim (\sim d) \equiv d$

Solution 1: I could just construct the truth table for both the cases and we would see that they are equivalent. However this time I will explain it in words. There are two logical possibilities, $\sim d$ is false and so $\sim (\sim d)$ is true. Also, when d is false, $\sim d$ is true and so $\sim (\sim d)$ is false. Therefore d and $\sim (\sim d)$ have the same truth values and are equivalent.

Problem 2: Prove $\sim (d \vee \sim k) \equiv \sim d \wedge k$

Solution 2: Let us use the newly introduced De Morgan's laws to prove this:

$$\sim (d \vee \sim k) \equiv \sim d \wedge k \tag{1.4.5}$$

But we know that $\sim (\sim k) \equiv k$, therefore:

$$\sim (d \vee \sim k) \equiv \sim d \wedge k \tag{1.4.6}$$

Problem 3: Prove $\sim (\sim d \wedge k) \equiv d \vee \sim k$

Solution 3: Once again applying De Morgan's laws:

$$\begin{aligned} \sim (\sim d \wedge k) &\equiv \ \sim (\sim d) \vee \sim k \\ &\equiv \ d \vee \sim k \end{aligned} \tag{1.4.7}$$

Problem 4: Prove $\sim (\sim d \vee \sim k) \equiv d \wedge k$

Solution 4: Applying De Morgan's laws:

$$\begin{aligned} \sim (\sim d \vee \sim k) &\equiv \ \sim (\sim d) \wedge \sim (\sim k) \\ &\equiv \ d \wedge k \end{aligned} \tag{1.4.8}$$

Example 10

Problem 1: Let us define the following statements;

d = He is honest

k = He is hard working

Give a verbal translation for the following compound statement $\sim (d \wedge k)$.

Solution 1: $d \wedge k$ means ”‘ He is both honest and hard working”’. So $\sim (d \wedge k)$ will mean ”‘It is not true that he is both honest and hard working”’. In other words we might be either honest or hard working which is equivalent to:

$$\sim d \vee \sim k \tag{1.4.9}$$

that is obtained using De Morgan's laws.

Problem 2: Now find a verbal translation for $\sim (d \vee k)$

Solution 2: $d \vee k$ means he is either honest or hard working. Therefore $\sim (d \vee k)$ means ”‘he is neither honest nor hard working”’, which is equivalent to the compound statement using De Morgan's laws:

$$\sim (d \vee k) \equiv \sim d \wedge \sim k \tag{1.4.10}$$

1.5 Conditional statements

Now lets discuss the connectives which we have not used till now, $\Rightarrow$ and $\Leftrightarrow$. Consider the statement; ”‘If you work had you will be successful”’. We can break it up into two sentences:

d = You must work hard

k = You will be successful

In symbols, the above compound statement can be written as:

$$d \Rightarrow k \tag{1.5.1}$$

Such statements are called *conditional* statements. Here k depends upon d, but d does not depend on k. The compound statement $d \Rightarrow k$ is true in every case except when d is true and k is false.

Example 11

Problem: Construct the truth table for $d \Rightarrow k$.

Solution: Truth table:

d	k	d $\Rightarrow k$
T	T	T
T	F	F
F	T	T
F	F	T

Table 9: Truth table for $d \Rightarrow k$

<u>Example 12</u>

Problem: Suppose;

d = The triangle is isosceles

and

k = Two sides of the triangle are of length

Translate the following compound statements into a symbolic form and give its equivalent statements in words and symbols;

Solution

The above compound statement in symbolic form:

$$d \Rightarrow k \tag{1.5.2}$$

We show that:

$$(d \Rightarrow k) \equiv \sim k \Rightarrow \sim d \tag{1.5.3}$$

The following truth table shows their equivalence:

d	k	d $\Rightarrow k$	$\sim d$	$\sim k$	$\sim k \Rightarrow \sim d$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

Table 10: Truth table showing $d \Rightarrow k \equiv \sim k \Rightarrow \sim d$

So, the equivalent statement in words will be "'If two sides of the triangle are not equal length then the triangle is not isosceles"'.

<u>Example 13</u>

Problem: Are the following statements equivalent; "'If the traders do not reduce the prices then the government will take action against them"', "'It is not true that the traders do not reduce the prices and governments does not take action against them"'.

Solution: Suppose;

d = traders do not reduce the prices

k = government takes action against them

The first statement in symbolic form:

$$d \Rightarrow k \tag{1.5.4}$$

and the second statement is:

$$\sim (d \wedge \sim k) \tag{1.5.5}$$

To prove this equivalence lets construct the truth table:

d	k	$\sim k$	d $\wedge \sim k$	$\sim (d \wedge \sim k)$	d $\Rightarrow k$
T	T	F	F	T	T
T	F	T	T	F	F
F	T	F	F	T	T
F	F	T	F	T	T

Table 11: Truth table showing $d \Rightarrow k \equiv \sim (d \wedge \sim k)$

1.6 Bi-conditional statements

Consider the statement;"'He will be successful if and only if he works hard"'. Now suppose we define:

d = He works hard

k = He is successful

Then the above compound statement in symbolic form:

$$d \Leftrightarrow k \tag{1.6.1}$$

Such statements are called *Bi-conditional statements.* The compound statement $d \Leftrightarrow k$ is true if and only if both $d \Rightarrow k$ and $d \Rightarrow k$ are true.

To see this lets construct the truth table:

d	k	d $\Rightarrow k$	k $\Rightarrow d$	d $\Leftrightarrow k$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	F	T

Table 12: Truth table for Bi-conditional statements

Example 15

Problem: A firm of chartered accountants makes the following declaration. A clerk from the firm passing the final C.A. examination in the first attempt will be awarded a prize of Rs 100. Five clerks, p, q, r, s, u appeared in the examination and only p, q could pass. The firm awards prizes not only to them, but also to r and s also. Is this action justified logically? u claims the prize comparing himself to r and s but the firm refuses. Is the refusal logically justified? How should the statement be worded so that only p and q will be entitled for the prize.

Solution: Suppose;

$$\text{d} = \text{passing the examination in first attempt}$$

$$\text{k} = \text{getting a prize}$$

Then the deceleration of the firm is a conditional statement:

$$d \Rightarrow k \tag{1.6.2}$$

From the truth table of $d \Rightarrow k$ we see that $d \Rightarrow k$ is false only when d is true and k is false. In other words if r and s get a prize, the action is logically justified by looking at the 3rd row of the truth table in example 11.

Again u does not get a prize implies q is false for u. Since "'u has not passed the examination at the first attempt"' implies that d false for u, so the 4th row suggests the action is logically justifies. Also p and q get a prize implies that k is true for p and q. Since p and q have passed the examination implies d us true for p and q. So, the first row suggests the action p and q getting a prize is logically justified.

Now consider the truth table of $d \Leftrightarrow k$ in Example 14. Since r, s, u fail in examination implies d is false for r, s, u. If they get a prize, then k is true for them. Third row suggests this is not correct. If r, s, u do not get a prize, then k is false for them and 4th row suggests it is correct, So, truth table of $d \Leftrightarrow k$ shows that if a person fails, he cannot get a prize.

Finally, if p, q get a prize, then d, k are true for both p and q and by the first row, it is correct. If p, q do not get a prize, then k is false for p and q and so by the second row, it is not true. So, the truth table of $d \Leftrightarrow k$ shows that only p and q can get a prize. Hence the statement should be; "'Only the people who pass the examination in the first attempt will get a prize of Rs 100"'.

Example 16

Problem: Are the following statements equivalent? (Justify)
"'It is not true that Darsh will get a job if and only if he secures first division."'
"'Darsh will not get a a job if and only if he secures first division."'

Solution: Suppose;

$$\text{d} = \text{Darsh gets a job}$$

$$\text{k} = \text{Darsh secures first division}$$

So in symbolic form:

$$\sim (d \Leftrightarrow k) \equiv \sim d \Leftrightarrow k \tag{1.6.3}$$

We prove this equivalence by constructing the truth table:

d	k	$\sim d$	$\sim d \Leftrightarrow k$	d $\Leftrightarrow k$	$\sim (d \Leftrightarrow k)$
T	T	F	F	T	F
T	F	F	T	F	T
F	T	T	T	F	T
F	F	T	F	T	F

Table 13: Truth table for $\sim (d \Leftrightarrow k) \equiv \sim d \Leftrightarrow k$

1.7 Tautology and contradiction

A statement is said to be a tautology if it is true for all logical possibilities. A statement is said to be a *contradiction* if it is false for all logical possibilities.

Example 17

Problem: Prove that the statement;

$$d \vee \sim d \tag{1.7.1}$$

is a tautology. While

$$d \wedge \sim d \tag{1.7.2}$$

is a contradiction.

Solution: If d is false then $\sim d$ is true. So, $d \vee \sim d$ is true and $d \wedge \sim d$ is false. Of d is true then $\sim d$ is false. So $d \vee \sim d$ is true and $d \wedge \sim d$ is false. These are all logical possibilities and in each case $d \vee \sim d$ is true while $d \wedge \sim d$ is false. This proves our assertion.

Example 18

Problem: Prove the following is a tautology;

$$(d \vee k) \Rightarrow (d \vee k) \tag{1.7.3}$$

Solution: Lets construct the truth table for the compound statement:

d	k	d $\wedge k$	d $\vee k$	(d $\vee k$) $\Rightarrow (d \vee k)$
T	T	T	T	T
T	F	F	T	T
F	T	F	T	T
F	F	F	F	T

Table 14: Truth table $(d \vee k) \Rightarrow (d \vee k)$

Example 19

Problem: Prove the following is a contradiction;

$$(d \wedge k) \wedge \sim (d \vee k) \tag{1.7.4}$$

Solution: Once again lets construct the truth table;

d	k	d $\wedge k$	d $\vee k$	$\sim (d \vee k)$	(d $\wedge k) \wedge \sim (d \vee k)$
T	T	T	T	F	F
T	F	F	T	F	F
F	T	F	T	F	F
F	F	F	F	T	F

Table 15: Truth table for $(d \wedge k) \wedge \sim (d \vee k)$

Since the compound statement, $(d \wedge k) \wedge \sim (d \vee k)$, has the truth value F for all logical possibilities it must be a contradiction.

Example 20

Problem: Prove the following is a tautology;

$$(d \Rightarrow k) \wedge (k \Rightarrow r) \Rightarrow (d \Rightarrow r) \tag{1.7.5}$$

Solution: Lets construct a truth table:
Where:

$$\alpha_1 = d \Rightarrow r \tag{1.7.6}$$

$$\alpha_2 = k \Rightarrow r \tag{1.7.7}$$

$$\alpha_3 = d \Rightarrow k \tag{1.7.8}$$

d	k	r	α_1	α_2	α_3	α_4	α_5
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	T
T	F	T	F	T	T	F	T
T	F	F	F	T	F	F	T
F	T	T	T	T	T	T	T
F	T	F	T	F	T	F	T
F	F	T	T	T	T	T	T
F	F	F	T	T	T	T	T

Table 16: Truth table for $(d \Rightarrow k) \wedge (k \Rightarrow r) \Rightarrow (d \Rightarrow r)$

$$\alpha_4 = (d \Rightarrow k) \wedge (k \Rightarrow r) \tag{1.7.9}$$

$$\alpha_5 = (d \Rightarrow k) \wedge (k \Rightarrow r) \Rightarrow (d \Rightarrow r) \tag{1.7.10}$$

Once again we see that the compound statement is True for all logical possibilities hence it is called a tautology.

Example 21

Problem 1: If d denotes tautology (i.e a statement that is always true) and k is any statement, then prove :

$$p \wedge t \equiv p \tag{1.7.11}$$

Solution 1: When k is true, $k \wedge d$ is also true (as t is always true) and when k is false, $k \wedge d$ is false. So, k and $k \wedge d$ and d are equivalent statements.

Problem 2: Now prove;

$$k \vee d \equiv d \tag{1.7.12}$$

Solution 2: When k is true, $k \vee d$ is also true and when k is false, $k \vee d$ is true. So, $k \vee d$ is always true. Hence $k \vee d$ and d are equivalent statements.

Example 22

Problem 1: If d denotes a contradiction (i.e a statement that is always false) and k be any statement, then prove:

$$k \vee d \equiv k \tag{1.7.13}$$

Solution 1: If k is true then $k \vee d$ is clearly true and if k is false, then $k \vee d$ is false (as d is always false). So, $k \vee d$ and k are equivalent statements.

Problem 2: Now prove;

$$k \wedge d \equiv d \tag{1.7.14}$$

Solution 2: If k is true then $k \wedge d$ is false and again k is false implies $k \wedge d$ is false. So, $k \wedge d$ is a contradiction. Hence $k \wedge d$ and d are equivalent statements.

1.8 Algebra of statements

There are certain laws that are defined algebraically that statements follow.

1.8.1 Commutative law

If d and k are two statements, then:

$$d \vee k \equiv k \vee d \tag{1.8.1}$$

$$d \wedge k \equiv k \wedge d \tag{1.8.2}$$

The proof is obvious and can be shown by constructing a truth table.

1.8.2 Associative law

If d, k, r are three statements then:

$$(d \vee k) \vee r \equiv d \vee (k \vee r) \tag{1.8.3}$$

$$(d \wedge k) \wedge r \equiv d \wedge (k \wedge r) \tag{1.8.4}$$

To prove it, let's construct the truth table:

d	k	r	α_1	α_2	α_3	α_4	α_5	α_6	α_7	α_8
T	T	T	T	T	T	T	T	T	T	T
T	T	F	T	T	T	F	T	T	T	T
T	F	T	T	T	F	F	T	T	F	F
T	F	F	T	F	F	F	T	T	F	F
F	T	T	T	T	F	T	T	T	F	F
F	T	F	T	T	F	F	T	T	F	F
F	F	T	F	T	F	F	T	T	F	F
F	F	F	F	F	F	F	F	F	F	F

Table 17: Truth table showing the associative law

Where:

$$\alpha_1 = d \lor k \tag{1.8.5}$$

$$\alpha_2 = k \lor r \tag{1.8.6}$$

$$\alpha_3 = d \land k \tag{1.8.7}$$

$$\alpha_4 = k \land r \tag{1.8.8}$$

$$\alpha_5 = (d \lor k) \lor r \tag{1.8.9}$$

$$\alpha_6 = d \lor (k \lor r) \tag{1.8.10}$$

$$\alpha_7 = (d \lor k) \lor r \tag{1.8.11}$$

$$\alpha_8 = d \land (k \land r) \tag{1.8.12}$$

Since the last two columns are equivalent we have completed the proof.

1.8.3 Identity law

If d denotes a tautology and k denotes a contradiction, then for any statement p:

$$p \lor d \equiv d \tag{1.8.13}$$

$$p \land s \equiv p \tag{1.8.14}$$

$$p \lor k \equiv p \tag{1.8.15}$$

$$p \land k \equiv k \tag{1.8.16}$$

Proof is given by constructing a truth table and is done in examples 21 and 22.

1.8.4 Complement law

For any statement p and tautology d and contradiction k;

$$p\vee \sim p \equiv d \tag{1.8.17}$$

$$p\wedge \sim p \equiv k \tag{1.8.18}$$

Proof is given by the truth table in example 17.

1.8.5 Distributive law

If d, k, r are three statements, then we can prove:

$$d \wedge (k \vee r) \equiv (d \wedge k) \vee (k \wedge r) \tag{1.8.19}$$

$$d \vee (k \wedge r) \equiv (d \vee k) \wedge (p \wedge r) \tag{1.8.20}$$

Once again the proofs are given by constructing truth tables:

d	k	r	α_1	α_2	α_3	α_4	α_5
T	T	T	T	T	T	T	T
T	T	F	T	F	T	T	T
T	F	T	F	T	T	T	T
T	F	F	F	F	F	F	F
F	T	T	F	F	T	F	F
F	T	F	F	F	T	F	F
F	F	T	F	F	T	F	F
F	F	F	F	F	F	F	F

Table 18: Truth table for $d \wedge (k \vee r) \equiv (d \wedge k) \vee (k \wedge r)$

Where:

$$\alpha_1 = k \wedge r \tag{1.8.21}$$

$$\alpha_2 = d \vee k \tag{1.8.22}$$

$$\alpha_3 = d \vee r \tag{1.8.23}$$

$$\alpha_4 = d \vee (k \wedge r) \tag{1.8.24}$$

$$\alpha_5 = (d \vee k) \wedge (d \vee r) \tag{1.8.25}$$

Since the last two columns are the same, we have proven that the statements are equivalent.
Where:

$$\alpha_1 = k \wedge r \tag{1.8.26}$$

d	k	r	α_1	α_2	α_3	α_4	α_5
T	T	T	T	T	T	T	T
T	T	F	F	T	T	T	T
T	F	T	F	T	T	T	T
T	F	F	T	T	T	T	T
F	T	T	T	T	T	T	T
F	T	F	F	T	F	F	F
F	F	T	F	F	T	F	F
F	F	F	T	F	F	T	T

Table 19: Truth table for $d \vee (k \wedge r) \equiv (d \vee k) \wedge (p \wedge r)$

$$\alpha_2 = d \vee k \tag{1.8.27}$$

$$\alpha_3 = d \vee r \tag{1.8.28}$$

$$\alpha_4 = d \vee (k \wedge r) \tag{1.8.29}$$

$$\alpha_5 = (d \vee k) \wedge (k \vee r) \tag{1.8.30}$$

Since the last two columns are the same, we have proved that the statements are equivalent.

1.8.6 Idempotent law

For any statement d:

$$d \vee d \equiv d \tag{1.8.31}$$

$$d \wedge d \equiv d \tag{1.8.32}$$

Proof can be given by constructing the tables, but it is also quite obvious.

1.8.7 De Morgan's laws

If d and k are two statements then:

$$\sim (d \wedge k) \equiv \sim d \vee \sim k \tag{1.8.33}$$

$$\sim (d \vee k) \equiv \sim d \wedge \sim k \tag{1.8.34}$$

We have already seen this and is proven in example 8.

1.8.8 Contrapositive law

For any statements d and k:

$$(d \Rightarrow k) \equiv (\sim k \Rightarrow \sim d) \tag{1.8.35}$$

Proof is given in example 12.

1.8.9 Law of double negation

For any statement d;

$$\sim (\sim d) \equiv d \tag{1.8.36}$$

Proof given in example 9.

1.8.10 Transitive law

For any statements d, k, r;

$$(d \Rightarrow k) \wedge (k \Rightarrow r) \Rightarrow (d \Rightarrow r) \tag{1.8.37}$$

is a tautology. Proof is given in example 20.

1.8.11 Law of addition

If d and k are two statements, then:

$$d \Rightarrow (d \vee k) \tag{1.8.38}$$

The proof can be seen by the construction of the truth table:

d	k	d $\vee k$	d $\Rightarrow (d \vee k)$
T	T	T	T
T	F	T	T
F	T	T	T
F	F	F	T

Table 20: Truth table for $d \Rightarrow (d \vee k)$

1.8.12 Law of simplification

:
If d and k are true statements then:

$$d \wedge k \Rightarrow d \tag{1.8.39}$$

$$d \wedge k \Rightarrow k \tag{1.8.40}$$

are both tautologies. The proof is similar to the previous truth table.

1.9 Deductive reasoning

The 12 laws listen in the "'Algebra of statements"' are very useful tools for proving the equivalence of different statements. In this section, we shall prove the equivalence of statements by using these laws only. The method of proof being used is called *deductive reasoning.*

Example 23

Problem: Prove the following tautology by deductive method:

$$d \wedge (d \Rightarrow k) \Rightarrow k \tag{1.9.1}$$

Solution: Firstly lets assume the following equivalence:

$$(d \Rightarrow k) \equiv \sim (d \wedge \sim k) \tag{1.9.2}$$

Proof is given in example 13. Now:

$$\begin{aligned}
p \wedge (p \Rightarrow k) \Rightarrow k &\equiv \sim ((d \wedge (d \Rightarrow k)) \wedge \sim k) \\
&\equiv \sim ((d \wedge \sim (d \wedge \sim k)) \wedge \sim k) \\
&\equiv \sim ((d \wedge (\sim d \vee k)) \wedge \sim k) \quad \text{De Morgans laws and double negation} \\
&\equiv \sim (((d \wedge \sim d) \vee (d \wedge k)) \wedge \sim k) \quad \text{Distributive law} \\
&\equiv \sim (((c \vee (d \wedge k)) \wedge \sim k) \quad \text{Complement law} \\
&\equiv \sim ((d \wedge k) \wedge \sim k) \quad \text{Identity law} \\
&\equiv \sim (d \wedge (k \wedge \sim k)) \quad \text{Associative law} \\
&\equiv \sim (d \wedge c) \quad \text{Complement law} \\
&\equiv \sim c \\
&\equiv t \qquad (1.9.3)
\end{aligned}$$

where c stands for a contradictive statement and t stands for a tautological statement. Therefore $p \wedge (p \Rightarrow k) \Rightarrow k$ is a tautology.

Example 24

Problem: Prove by deductive reasoning that the following is a tautology:

$$(d \vee k) \vee \sim d \Rightarrow k \qquad (1.9.4)$$

Solution: Once again we use the definition used in example 23:

$$\begin{aligned}
(d \vee k) \vee \sim d \Rightarrow k &\equiv \sim (((d \vee k) \vee \sim d) \wedge \sim k) \\
&\equiv \sim (((d \wedge \sim d) \vee (k \wedge \sim d)) \wedge \sim k) \quad \text{Distributive law} \\
&\equiv \sim ((c \vee (k \wedge \sim d)) \wedge \sim k) \quad \text{Complement law} \\
&\equiv \sim ((d \wedge \sim k) \wedge \sim k) \quad \text{Identity law} \\
&\equiv \sim ((\sim d \wedge k) \wedge \sim k) \quad \text{Commutative law} \\
&\equiv \sim (\sim d \wedge (k \wedge \sim k)) \quad \text{Associative law} \\
&\equiv \sim (\sim d \wedge c) \quad \text{Complement law} \\
&\equiv \sim c \quad \text{Identity law} \\
&\equiv t \qquad (1.9.5)
\end{aligned}$$

Therefore $(d \vee k) \vee \sim d \Rightarrow k$ is a tautology.

1.10 Argument

An argument is the assertion that a statement, called a *conclusion*, follows from other statements, called *hypothesis*. For example consider the following statements;

If he works hard he will be successful

He was not successful

Therefore he did not work hard

These three statements, taken together form an argument in which the first two statements are hypothesis and the last statement is the conclusion. Now consider the argument; If:

d = He works hard

k = He is successful

this argument can written symbolically as:

$$(d \Rightarrow k) \wedge \sim k \Rightarrow \sim k \tag{1.10.1}$$

If an argument is a tautology, we say it is a *valid argument*. If it is not a tautology (does not mean it is a contradiction!), it is said to be an *invalid* argument.

Example 25

Problem: Prove that the following argument is valid. "'If he works hard, he will be successful. He was not successful. Therefore, he did not work hard"'.

Solution: Suppose

d = He works hard

k = He is successful

The argument can then be written as:

$$(d \Rightarrow k) \wedge \sim k \Rightarrow \sim k \tag{1.10.2}$$

To prove this lets construct the truth table:

d	k	$\sim d$	$\sim k$	α_1	α_2	α_3
T	T	F	F	T	F	T
T	F	F	T	F	F	T
F	T	T	F	T	F	T
F	F	T	T	F	T	T

Table 21: Truth table for $(d \Rightarrow k) \wedge \sim k \Rightarrow \sim k$

Where:

$$\alpha_1 = pk \tag{1.10.3}$$

$$\alpha_2 = (d \Rightarrow k) \wedge \sim k \tag{1.10.4}$$

$$\alpha_3 = (d \Rightarrow k) \wedge \sim q \Rightarrow \sim k \tag{1.10.5}$$

Since the argument is always true it is valid.

Example 26

Problem: Prove that the following argument is not valid. "'If it rains, crops will be good. It did not rain, therefore the crops were not good"'

Solution: Suppose:

d = It rains

Crops are good

Then the argument can be written as:

$$(d \Rightarrow k) \wedge \sim d \Rightarrow \sim k \tag{1.10.6}$$

Lets construct the truth table:

d	k	$\sim d$	$\sim k$	α_1	α_2	α_3
T	T	F	F	T	F	T
T	F	F	T	F	F	T
F	T	T	F	T	T	F
F	F	T	T	T	T	T

Table 22: Truth table for $(d \Rightarrow k) \wedge \sim d \Rightarrow \sim k$

Where:

$$\alpha_1 = d \Rightarrow k \tag{1.10.7}$$

$$\alpha_2 = (d \Rightarrow k) \wedge \sim k \tag{1.10.8}$$

$$\alpha_3 = (d \Rightarrow k) \wedge \sim k \Rightarrow \sim k \tag{1.10.9}$$

Since the last column is not always true the argument is not valid.

Example 27

Problem: Test the validity of the following statement; "'If my brother stands first in the class, I give him a watch. Either he stood first or I was out of station so I did not give my brother a watch this time. Therefore, I was out of station"'.

Solution: Suppose:

d = My brother was first

k = I gave him a watch

r = I was out of station

This can be written as:

$$(d \Rightarrow k) \wedge (d \vee r) \wedge (\sim k) \Rightarrow r \tag{1.10.10}$$

Once again this can be proven to be a tautology by constructing a truth table, however it would be very long and it similar to the previous ones so I will not do it here.

1.11 Joint denial

We introduce a new connective ”‘ $\downarrow$ ”$'$ called *joint denial.* If d and k are two statements; then $d \downarrow k$ will be read as ”‘neither d nor q”’. The compound statement $d \downarrow k$ is true if and only if both d and k are false. We will see that any compound statement which have connectives like $\wedge, \vee, \sim$ can all be replaced by a single connective, $\downarrow$. So, the resulting compound statement will have only, $\downarrow$, this comes in handy in the designing of a computer, as it is much simpler and economical to design a computer where only one operation is performed.

Example 28

Problem: Construct the truth table for the compound statement:

$$d \downarrow k \tag{1.11.1}$$

Solution:

d	k	d $\downarrow k$
T	T	F
T	F	F
F	T	F
F	F	T

Table 23: Truth table for $d \downarrow k$

Example 29

Problem: Prove the following statement is equivalent;

$$\sim d \equiv d \downarrow d \tag{1.11.2}$$

Solution:

d	$\sim d$	d $\downarrow d$
T	F	F
F	T	T

Table 24: Truth table for $\sim d \equiv d \downarrow d$

Example 30

Problem: Show that $d \downarrow k$ and $\sim d \wedge \sim k$ are equivalent.

Solution: The following truth table will prove this:

d	k	$\sim d$	$\sim k$	$\sim d \wedge \sim k$	d $\downarrow k$
T	T	F	F	F	F
T	F	F	T	F	F
F	T	T	F	F	F
F	F	T	T	T	T

Table 25: Truth table for $d \downarrow k \equiv \sim d \wedge \sim k$

Example 31

Problem 1: Prove:

$$(d \wedge k) \equiv (d \downarrow d) \downarrow (k \downarrow k) \tag{1.11.3}$$

Solution 1: Truth table;

d	k	d $\wedge k$	d $\downarrow d$	k $\downarrow k$	(d $\downarrow d) \downarrow (k \downarrow k)$
T	T	T	F	F	T
T	F	F	F	T	F
F	T	F	T	F	F
F	F	F	T	T	F

Table 26: Truth table for $(d \wedge k) \equiv (d \downarrow d) \downarrow (k \downarrow k)$

Since the third and last columns are the same they must be equivalent.

Problem 2: Prove;

$$(d \wedge k) \equiv (d \downarrow k) \downarrow (k \downarrow d) \tag{1.11.4}$$

Solution 2: Truth table;

d	k	d $\vee k$	d $\downarrow d$	(d $\downarrow k) \downarrow (k \downarrow d)$
T	T	T	F	T
T	F	T	F	T
F	T	T	F	T
F	F	F	T	F

Table 27: Truth table for $(d \wedge k) \equiv (d \downarrow k) \downarrow (k \downarrow d)$

Example 32

Problem: Give an equivalent statement of $d \Rightarrow k$ in terms of connectives $\downarrow$

only.

Solution: We know:

$$(d \Rightarrow k) \equiv \sim (d \wedge \sim k) \tag{1.11.5}$$

From example 29 we know:

$$\sim (d \wedge \sim k) \equiv (d \wedge \sim k) \downarrow (d \wedge \sim k) \tag{1.11.6}$$

By example 31 we know:

$$(d \wedge \sim k) \equiv (d \downarrow d) \downarrow (\sim k \downarrow \sim k) \tag{1.11.7}$$

Again from example 29:

$$\sim k \equiv k \downarrow k \tag{1.11.8}$$

Combining these three statements:

$$\begin{aligned}
(p \Rightarrow k) &\equiv \sim (d \wedge \sim k) \\
&\equiv (d \wedge \sim k) \downarrow (d \wedge \sim k) \\
&\equiv (d \downarrow d) \downarrow (\sim k \downarrow \sim k) \downarrow (d \downarrow d) \downarrow (\sim k \downarrow \sim k) \\
&\equiv (d \downarrow d) \downarrow ((k \downarrow k) \downarrow (k \downarrow k)) \downarrow (d \downarrow d) \downarrow ((k \downarrow k) \downarrow (k \downarrow k))
\end{aligned}$$

1.12 Inverting truth tables

In the preceding sections we have been constructing the truth table for a given compound statement. It is also interesting to consider the converse problem. Given a truth table to find one or more compound statements.

Example 33

Problem: Construct one or more compound statements given the following truth table:

d	k	r	?
T	T	T	T
T	T	F	F
T	F	T	T
T	F	F	F
F	T	T	F
F	T	F	F
F	F	T	T
F	F	F	F

Table 28: Truth table with a statement missing

Solution: There is no set method to find the answer from the truth tables (as far as I know). However an easy way is to simply look at the entries in the column which we are to determine the statement of. For example there are three T's in the last column. The statement:

$$d \wedge k \wedge r \tag{1.12.1}$$

satisfies the first row. The statements:

$$d \wedge \sim k \wedge r \tag{1.12.2}$$

and

$$\sim d \wedge \sim k \sim r \tag{1.12.3}$$

satisfy the third and seventh row respectively. Therefore I can construct a statement:

$$(d \wedge k \wedge r) \vee (d \wedge \sim k \wedge r) \vee (\sim d \wedge \sim k \wedge r) \tag{1.12.4}$$

Which will satisfy the last column of the truth table. Infact this is a method that will always work. One simply finds the statement that satisfy the row with the 'T' entry and then combine them using the "'or"', ∨ connective. The compound statement found in this way will not be the most concise, however further work can be done on it by using deductive reasoning.

Example 34

Problem: Construct one or more compound statements for the following truth table:

d	k	?
T	T	T
T	F	F
F	T	F
F	F	T

Table 29: Truth table with a statement missing

Solution: The first row is clearly satisfied by the statement:

$$(d \wedge k) \vee (\sim d \wedge \sim k) \tag{1.12.5}$$

Using deductive reasoning this can be reduced to:

$$d \Rightarrow k \tag{1.12.6}$$

Example 35

Problem: A student is confronted with a true-false exam, consisting of five questions. He knows that his instructor always has more true then false questions and he never has three questions in a row with the same answer. From the nature of the first and last question he knows that these must have the opposite answers. The only question to which he knows the answer is number two and this assures him of having all answers correct. What did he know about question two? What are the answers to the five questions?

Solution: It is easy to see that three questions have answers 'True' and two are 'False'. Let:

$$\text{d} = \text{The answer to question 3 is true}$$

$$\text{k} = \text{The answer to question 4 is true}$$

Now suppose the answer to question number 2 is true. Then d is true (because if d is false, then there will be two correct answers; TTFTF and FTFTT. This is not possible as the answer to question 2 assumes him of having all the answers correct). Similarly, if the answer to question 2 is false, then d is false. So we get the following truth table:

d	Answer to Q2
T	True
F	False

Table 30: Truth table in which T and F indicate the truth values of d

Again if the answer to question 2 is true, then truth value of k is either T or F. If truth value of d is T, then there will be two correct answers namely TTFTF and FTFTT. This is not possible, so the truth value of the resulting statement is F. Again, if truth value of k is F, then there will be only one correct answer, namely FTTFT. So, the truth value of the resulting statement will be F (whatever the truth value of k may be). So, we have the following truth table:

d	k	Answer to Q2	?
T	T	True	F
T	F	True	T
F	T	False	F
F	F	False	F

Table 31: Truth table for Answer to Q2 with the missing statement

The statement $d\wedge \sim k$ has the truth table as above. So, the student finds that the answer to question 3 is true and to question 4 is false. This shows that the answer to question 5 is true which in turn means that the answer to question 1 is false. Therefore the answer to question 2 is true.

1.13 Application: Circuits

We will now discuss how the theory of compound statements can be applied in Electrical engineering. As an example, a theory of simple switching networks is developed. A switching network is an arrangement of wires and switches which connects together two terminals T_1 and T_2. Each switch has two states 'open' and 'close'. A closed switch allows the current to pass and an open switch does not.

As a basic example, consider:

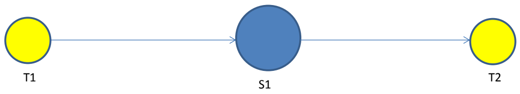

Figure 1: Simple circuit showing two terminals and a switch

I will follow the notation where T and S in figures will stand for terminals and switches. If any other components are used, then they will also be represented similarly. In this example the terminals are connected by a single wire containing a switch S1. If S1 is closed, then the current will flow between the terminals. Now suppose we have:

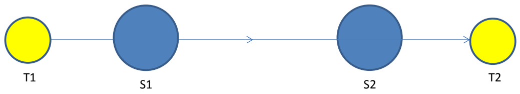

Figure 2: Circuit showing two terminals and two switches in series

The network has two switches S1 and S2 in series. The current will flow when both S1 and S2 are closed.

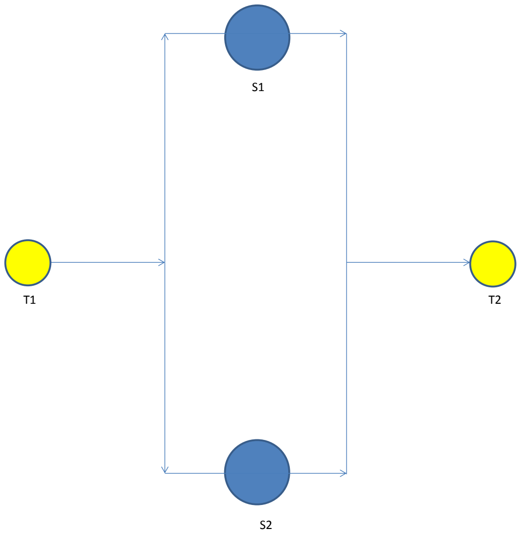

Figure 3: Circuit showing two switches in parallel

In figure 3, switches S1 and S2 are placed in parallel. This simply means that the current will flow if any one of S1 and S2 is closed. We now see how the theory of logic can explain the networks shown in the figures above. Let's define:

d = S1 is closed

k = S2 is closed

Then in the first network, current will flow if and only if d is true. In the second network, the current will flow if and only if k is true. In the second network, current will flow if and only if both d and k are true and network 3 shows that current will flow if and only if at least one of the statements d or k is true. The network in the first figure can be represented by the statement d. Network two is represented by a compound statement:

$$d \wedge k \tag{1.13.1}$$

and network 3 is:

$$d \vee k \tag{1.13.2}$$

It is possible that two (or more) switches may be linked together so that they may open or close simultaneously. We denote these switches by the same letters in the diagrams. If we represent two switches by letters S1 and S1' then it means whenever S1 is open S1' is closed and conversely. Consider the following network of switches:

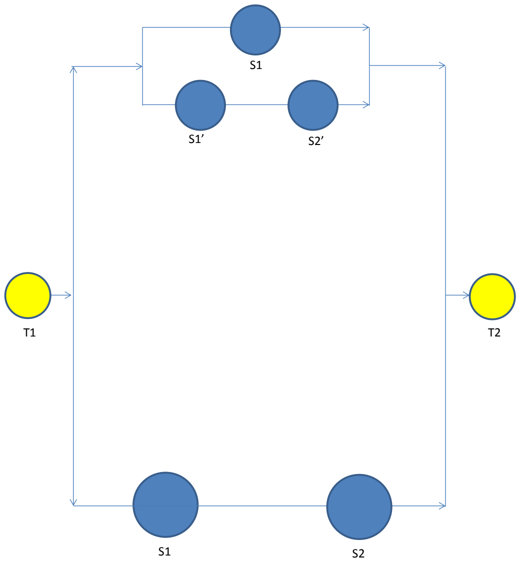

Figure 4: Network of switches in both parallel and series

If:

d = Switch S1 is closed

k = Switch S2 is closed

then the network in the figure above may be expressed in symbolic form of logic as:

$$d \vee (\sim d \wedge \sim k) \wedge (d \wedge k) \tag{1.13.3}$$

It is very clear from the figure that current will flow if and only if the compound statement is true. There are also switching networks which are placed in series. For example:

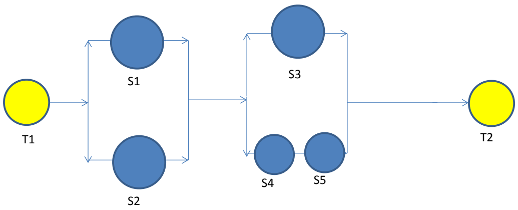

Figure 5: Two network of switches in series.

The compound statement can be written as:

$$(d \vee k) \wedge (r \vee (s \wedge t)) \tag{1.13.4}$$

Where:

d = Switch S1 is closed

k = Switch S2 is closed

r = Switch S3 is closed

s = Switch S4 is closed

t = Switch S5 is closed

Example 36

Problem: Give an alternate arrangement of the following network such that the new network has two switches:

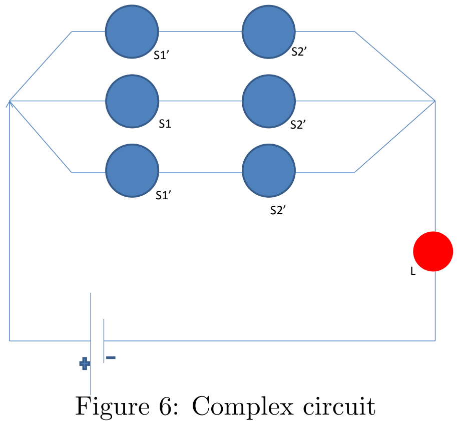

Figure 6: Complex circuit

Here L stands for light.

Solution: The given network may be expressed as:

$$(\sim d \wedge \sim k) \vee (d \wedge \sim k) \wedge (\sim d \wedge k) \tag{1.13.5}$$

Now using deductive reasoning we can formulate a simpler version of the circuit:

$$\begin{aligned}(\sim d \wedge \sim k) \wedge (d \wedge \sim k) \wedge (\sim d \wedge k) &\equiv (\sim d \wedge \sim k) \wedge (\sim k \wedge d) \wedge (\sim d \wedge k)\\ &\equiv (\sim k \wedge (\sim d \wedge d)) \vee (\sim d \wedge k)\\ &\equiv \sim k \vee (\sim d \wedge k)\\ &\equiv (\sim k \vee \sim d) \wedge (\sim k \wedge k)\\ &\equiv (\sim k \vee \sim k) \qquad (1.13.6)\end{aligned}$$

So here we see the real power of the framework of logic applied to circuits.

Therefore an alternative circuit is two open switches in parallel:

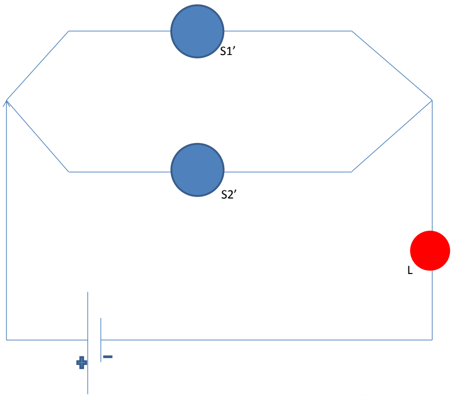

Figure 7: Equivalent circuit to figure 6.

Example 37

Problem: This time, let us consider a network with 10 switches. We have to find an alternate arrangement with two switches only:

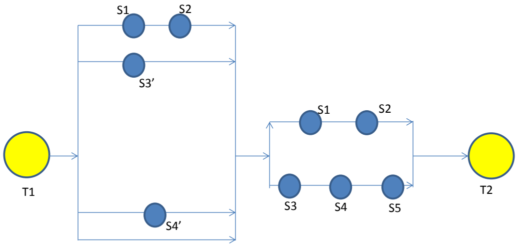

Figure 8: Two networks with series and parallel switches inside, in series with each other.

Solution: Let d, k, r, s, t stand for 'Switch S1 to S5 are closed' respectively, then the given network may be expressed as the following compound statement:

$$\begin{aligned}((d \wedge k) \vee (\sim r \vee \sim s \vee \sim t)) \wedge ((d \wedge k) \vee (r \wedge s \wedge t)) &\equiv (d \wedge k) \vee ((\sim r \vee \sim s \vee \sim t) \wedge (r \wedge s \wedge t)) \\ &\equiv (d \wedge k) \vee (\sim (r \wedge s \wedge t) \wedge (r \wedge s \wedge t)) \\ &\equiv (d \wedge k) \qquad (1.13.7)\end{aligned}$$

So we are led to the following, very simple, network:

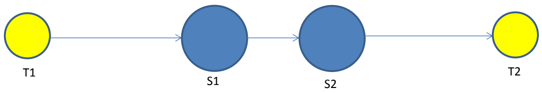

Figure 9: Alternative to figure 8

Note that in this problem there are two networks which have been placed in series.

Example 38

Problem: Now let's try to work backwards and construct a network for the following statement:

$$(d \wedge k \wedge \sim r) \vee (\sim d \wedge (k \wedge \sim r)) \tag{1.13.8}$$

Solution: Lets break the statement down into smaller statements; Firstly, $d \wedge k \wedge \sim r$ is a network in series which is parallel to $\sim d \wedge (k \wedge \sim r)$, which in itself has $\sim d$ is series with $k \vee \sim r$. Now the network can be drawn as:

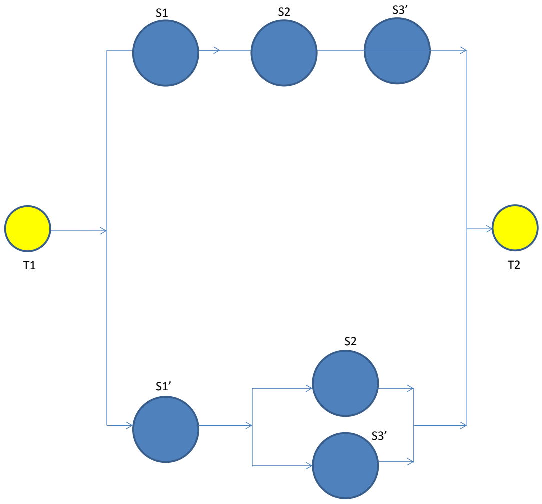

Figure 10: Network for equation 1.13.8

Example 39

Problem: Give an alternate arrangement of the following network such that the new arrangement has only five switches:

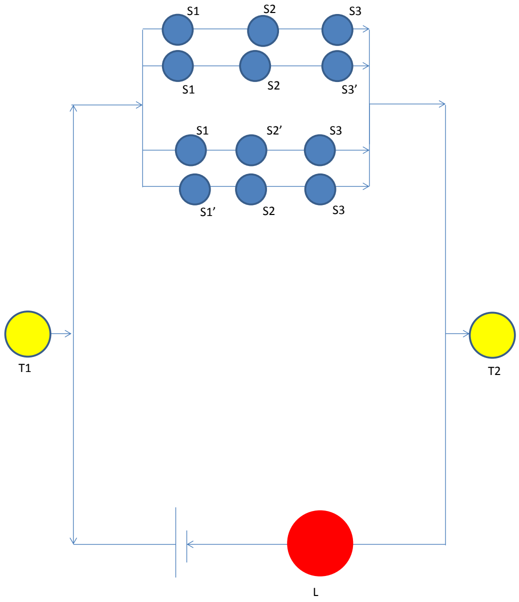

Figure 11: Network that needs to be changed

Solution: Let us express the network as a statement, by letting $d \wedge k \wedge r$ meaning the usual statements:
$(\mathrm{d} \wedge k \wedge r) \vee (d \wedge k \wedge r) \vee (d \wedge k \wedge r) \vee (\sim d \wedge k \wedge r) \equiv ((d \wedge k \wedge r) \vee (d \wedge k \wedge \sim r) \vee ((d \wedge k \wedge r) \wedge (d \wedge \sim k \wedge r)) \vee ((p \wedge q \wedge r)(\sim d \wedge k \wedge r))$
$\equiv ((d \wedge k) \vee (r \vee \sim r)) \vee ((d \wedge r) \wedge (k \wedge \sim k)) \vee ((k \vee r) \wedge (d \vee \sim d))$
$\equiv (d \vee k) \vee (d \wedge r) \vee (k \vee r)$
$\equiv (d \wedge (k \vee r)) \vee (k \wedge r)$

In this equivalent statement, there are only five switches as required.

This equivalent statement may be expressed by the following network:

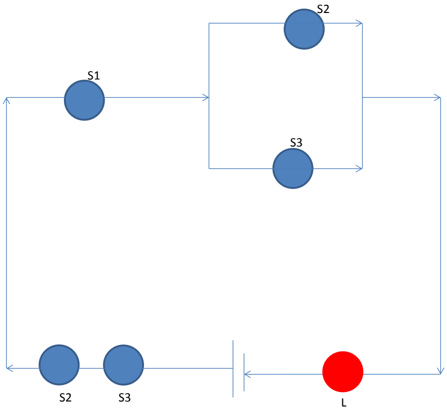

Figure 12: Alternative to figure 11

<u>Example 40</u>

Problem: Suppose we want to design the following game; At a given signal, two players, A and B, open or close a switch under the control. If they both do the same, A wins; if they do the opposite the B wins. Design the circuit so that the light does on if A wins.

Solution: Suppose:

d = A opens switch

k = B opens switch

We know that the light goes on when both d and k are true or both p and q are false and also conversely. The circuit can therefore we written as:

$$(d \wedge k) \vee (\sim d \wedge \sim k) \tag{1.13.8}$$

Which is given as:

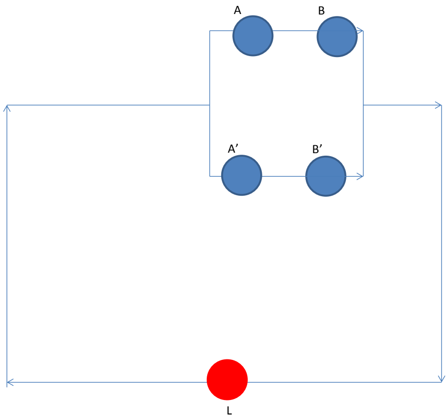

Figure 13: Network for the game where A and B are the players

2 Set Theory

2.1 Sets

Sets are the most fundamental objects in mathematics. Almost anything one can think of falls in the category of some form of set. This was first formulated by Georg Cantor. Set theory can be developed axiomatically, but here we shall develop the theory of how sets relate to each other, without the axiomatic definition of a set.

An axiomatic approach is taken in plane geometry, where we prove theorems about points and lines without precise definitions of these terms. We shall therefore content ourselves by accepting the following definition of a set: *A set is any collection of objects such that given an object, it is possible to determine weather that object belongs to the given collection of not*

Example 1

1: The set of all integers *2*: The set of all the people living in Milton Keynes. *3*: The set of all the letters in the alphabet. *4*: The set of even integers

Example 2

Problem: Let M be the collection of all the men in a village who do not shave themselves. Given that **i)** All men in the village must be clean shaven **ii)** The village barber shaves all those men who do not shave themselves. Is M a set?

Solution: Suppose b denotes the village barber. If b belongs to M (i.e he does not shave himself) then the statement **ii)** means we have a contradiction. As the barber belongs to M, therefore he cannot shave himself and **ii)** states that all the people who do not shave themselves are shaven by b.

Now suppose b does not belong to M, then b shaves himself. Then by **ii)** b does not shave himself, which again leads to a contradiction. Since we cannot answer Yes or No to the question; 'Is barber himself a member of M?' we conclude that M is not a set.

The members of a set are called elements. We shall use capital letters to denote sets and small letters to denote elements. If d is an element of the set D, we write:

$$d \in D \tag{2.1.1}$$

which is read as 'd belongs to D'. If d is not an element of the set D, we write:

$$d \notin D \tag{2.1.2}$$

which is read as 'd does not belong to D'. There are different ways od describing a set. For example, the set consisting of elements 1,2,3,4,5 could be written as:

$$\{1,2,3,4,5\} \quad \text{or} \quad \{1,2...5\} \quad \text{or} \quad \{x|x \in N, x \leq 5\} \tag{2.1.3}$$

where N is the set of Natural numbers, we use {} to denote a set. A set which has a finite number of elements is called a finite set. Otherwise, it is called an infinite set. For example, if D is the set of all integers, then D is an infinite set denoted by:

$$\{..., -2, -1, 0, 1, 2, ...\} \quad \text{or} \quad \{x| \;\; x \;\text{ is an integer}\} \tag{2.1.4}$$

A set having only one element is called a *Singleton*. If d is the element of the singleton D, then D can be written as:

$$D = \{d\} \tag{2.1.5}$$

Note that $\{d\}$ and d do not mean the same thing; $\{d\}$ stands for the set containing a single element, while d is just an element of $\{d\}$ (albeit it is the only element).

2.2 Equality of sets

Two sets D and K are said to be equal if and only if every member of D is a member of K and every member of K is a member of D (note that it is important to state the second statement as the opposite arguement is not mutually inclusive). We express this by:

$$D = K \tag{2.2.1}$$

logically speaking, this means:

$$(x \in D) \equiv (x \in K) \tag{2.2.2}$$

or the bi-conditional statement:

$$(x \in D) \Leftrightarrow (x \in K) \quad \text{true for all x} \tag{2.2.3}$$

The order of the elements in a set is irrelevant. For example, the sets;

$$\{1, 2, 3\} = \{2, 3, 1\} = \{3, 2, 1\} \tag{2.2.4}$$

We always write each element of a set only once. For example, $\{2, 2, 3\}$ is not a proper way of presenting a set. This should be written as $\{2, 3\}$.

2.3 Subsets

Let D and K be two sets. If every element of D is an element of K then D is called a subset of K and we write:

$$D \subseteq K \;\; \text{or} \;\; K \supseteq D \tag{2.3.1}$$

read as 'D is contained in K' or 'K contains D'. In logical terms; $D \subseteq K$ stands for:

$$(x \in D) \Rightarrow (x \in K) \quad \text{true for all x} \tag{2.3.2}$$

If $D \subseteq K$ and $D \neq K$ we write:

$$D \subset K \quad \text{or} \quad K \supset D \tag{2.3.3}$$

read as 'D is a *proper* subset of K' or 'K is a *proper* super-set of D'. In fact every set is a subset and super-set of itself. If D is not a subset of K, we can write it as:

$$D \nsubseteq K \tag{2.3.4}$$

2.4 Null set

A set which does not contain any elements is called the null set. It is usually denoted by the symbol of $\emptyset$.

Example 3

Each of the following is a null set:
1: The set of all real numbers whose square is -1
2: The set of all integers that are both odd and even.
3: The set of all rational numbers whose square is 2
4: The set of all integers, x, that satisfy the equation $2x = 13$

Example 4

Problem: Prove that the null set (empty set) $\emptyset$ is a subset of every set.

Solution: Suppose $\emptyset$ is not a subset of the set D. This means there exists:

$$d \in \emptyset \tag{2.4.1}$$

such that:

$$d \notin D \tag{2.4.2}$$

This is impossible as $\emptyset$ has no elements. Therefore, $\emptyset$ must be a subset of every set. In terms of logic, we want to prove the conditional statement:

$$(x \in \emptyset) \Leftarrow (x \in D) \tag{2.4.3}$$

is true for every x. Since $\emptyset$ has no elements, the statement:

$$x \in \emptyset \tag{2.4.4}$$

is false. So the conditional statement in Eq 2.4.3 is true, which proves the result.

Example 5

Problem 1: List the elements of set:

$$\{x|x \in N \quad \text{and} \quad x \leq 9\} \tag{2.4.5}$$

Solution 1: N stands for natural numbers. We have to find the natural numbers which are one less than 10. They are 1,2,3,4,5,6,7,8,9. Therefore the set is:

$$D = \{1, 2, 3, 4, 5, 6, 7, 8, 9\} \tag{2.4.6}$$

Problem 2: List the elements of set:

$$\{x|x \in Z \quad \text{and} \quad x \leq 5\} \tag{2.4.7}$$

Solution 2: Z stands for the set of integers. We have to find the integers which are less than 6:

$$D = \{-5, -4, -3, -2, ...2, 3, 4, 5\} \tag{2.4.8}$$

Problem 3: List the elements of the set:

$$\{x|x \in Z \quad \text{and} \quad 2 < x <\} \tag{2.4.9}$$

Example 6

Problem 1: Give the verbal translation of the following set:

$$D_1 = \{2, 4, 6, 8\} \tag{2.4.10}$$

Solution 1: D$_1 isasetthatcontainsall, positive, evenintegersbetween0and10$.

Problem 2: Give the verbal translation of the following set:

$$D_2 = \{1, 3, 5, 7, 9, ...\} \tag{2.4.11}$$

Solution 2: D$_2 isasetofallpositive, odd, integers$.

Problem 3: Give the verbal translations of the following set:

$$D_3 = -1, 1 \tag{2.4.12}$$

Solution 3: D$_3 isasetofintegers, x, thatsatisfytheequation$:

$$x^2 - 1 = 0 \tag{2.4.13}$$

Example 7

Problem: If:

$$d_1 k_2 \tag{2.4.14}$$

and

$$\{d_1, k_1\} = \{d_2, k_2\} \tag{2.4.15}$$

then show that:

$$d_2 \neq k_2 \tag{2.4.16}$$

Solution: Let:

$$d_2 = k_2 \tag{2.4.17}$$

Then:

$$d_1 \in \{d_1, k_1\} \tag{2.4.18}$$

which also implies:

$$d_1 \in \{d_2, k_2\} \tag{2.4.19}$$

So, $d_1 = d_2$. Also:

$$k_2 \in \{d_1, k_1\} \tag{2.4.20}$$

means:

$$k_1 \in \{d_2, k_2\} = \{d_2\} \tag{2.4.21}$$

Therefore:

$$k_1 = d_2 \tag{2.4.22}$$

and

$$d_1 = k_1 \tag{2.4.23}$$

which is wrong, therefore:

$$d_2 \neq k_2 \tag{2.4.24}$$

Example 8

Problem: Prove:

$$D \subseteq K \quad \text{and} \quad K \subseteq C \quad \text{then} \quad D \subseteq C \tag{2.4.25}$$

solution: Let:

$$d \in D \tag{2.4.26}$$

to any element of D. Then as:

$$D \subseteq K, d \in K \tag{2.4.27}$$

Also;

$$K \subseteq C \Leftarrow d \in C \tag{2.4.28}$$

Thus every element of D belongs to $C \Leftarrow D \subseteq C$. In logical terms, we want to prove:

$$((x \in D) \Leftarrow (x \in K)) \wedge ((x \in K) \Leftarrow (x \in C)) \Leftarrow ((x \in D) \Leftarrow (x \in C)) \tag{2.4.29}$$

This follows from the transitive law given in the first chapter.

Example 9

Problem: Prove:

$$D \subseteq K \quad \text{and} \quad K \subseteq D \quad \text{then} \quad D = K \tag{2.4.30}$$

Solution: Since:

$$D \subseteq K \tag{2.4.31}$$

every element of D is an element of K. Also:

$$K \subseteq D \tag{2.4.32}$$

means every element of K is in D. This proves $D = K$. Logically speaking, we want to prove:

$$((x \in D) \Rightarrow (x \in K)) \wedge ((x \in K) \Rightarrow (x \in D)) \Rightarrow ((x \in D) \Leftrightarrow (x \in K)) \tag{2.4.33}$$

is true for all x. In other words:

$$((p \Rightarrow q) \wedge (q \Rightarrow p)) \Rightarrow (p \Leftrightarrow q) \quad \text{is true.} \tag{2.4.34}$$

Since:

$$p \Rightarrow q \tag{2.4.35}$$

is true and:

$$q \Rightarrow p \tag{2.4.36}$$

is true,

$$(p \Rightarrow p) \wedge (q \Rightarrow p) \tag{2.4.37}$$

is also true. This also means:

$$p \Leftrightarrow q \tag{2.4.38}$$

is true. So:

$$((q \Rightarrow q) \wedge (q \Rightarrow q)) \Rightarrow (p \Leftrightarrow p) \tag{2.4.39}$$

is true and this completes the proof.

Example 10

Problem: Prove:

$$D \subset K \quad \text{and} \quad K \subseteq C \quad \text{then} \quad D \subset C \tag{2.4.40}$$

Solution: Lets suppose:

$$D = C \tag{2.4.41}$$

Then every element of K is also an element of D (as $K \subseteq D$). But $D \subset K$ means every element of D is also an element of K. Combining these facts, we get:

$$D = K \tag{2.4.42}$$

which is a contradiction as D is a proper subset of K. So:

$$D \neq C \tag{2.4.43}$$

and every element of D is also an element of C. Therefore D, is a proper subset of C. In the logic formalism, $D \subset K$ means:

$$(x \in D) \Rightarrow (x \in K) \tag{2.4.44}$$

is true for all x. Therefore:

$$(x \in D) \Leftrightarrow (x \in D) \tag{2.4.45}$$

is true for every x. So

$$D = K \tag{2.4.46}$$

which is not possible as D is a proper subset of K, Thus $D \neq K$ and D is a subset of C.

Example 11

Problem 1: Find all possible solutions for x and y:

$$\{2x, y\} = \{4, 6\} \tag{2.4.47}$$

Solution 1: Let:

$$D = \{2x, y\} \quad \text{and} \quad K = \{4, 6\} \tag{2.4.48}$$

Now

$$2x \in D \tag{2.4.49}$$

means

$$2x \in K \tag{2.4.50}$$

So

$$2x = 4 \tag{2.4.51}$$

or

$$2x = 6 \tag{2.4.52}$$

If $2x = 4$ then $x = 2$. Also:

$$y \in D \tag{2.4.53}$$

means

$$y \in K \tag{2.4.54}$$

So, $y = 4$ or 6, y cannot be equal to 4. As then D will become:

$$\{4, 4\} = \{4\} \tag{2.4.55}$$

hence it will only have one element while K will have 4 and 6. Therefore the solution must be $x = 2$ and $y = 2$. Now if $2x = 6$, then $x = 3$ and y cannot be 6 as once again D will have only one element, 6. Therefore the only possible solution is $x = 3$ and $y = 4$ (remember the order of numbers does not matter).

Problem 2: Find all possible solutions for x and y:

$$\{x, 2y\} = \{1, 2\} \tag{2.4.56}$$

Solution 2: Lets define:

$$D = \{x, 2y\} \quad \text{and} \quad K = \{1, 2\} \tag{2.4.57}$$

Now:

$$x \in D \quad \text{means} \quad x \in K \tag{2.4.58}$$

So x = 1 or 2. If x = 1, then $2y = 2$. So one possible solution is $x = 1$ and $y = 1$. If $x = 2$, then $2y = 1$, so another solution is $x = 2$ and $y = 12$.

Problem 3: Find all possible solutions for x and y in:

$$\{2x\} = \{0\} \tag{2.4.59}$$

Solution 3: Lets define:

$$D = \{2x\} \quad \text{and} \quad K = \{0\} \tag{2.4.60}$$

Now:

$$2x \in D \quad \text{means} \quad 2x \in K \tag{2.4.61}$$

So, $2x = 0$ which has only one solution that $x = 0$.

Example 12

Problem: Find at least one set D such that:

$$\{1, 2\} \subseteq D \subset \{1, 2, 3, 4\} \tag{2.4.62}$$

Solution: Since

$$\{1, 2\} \subset D \tag{2.4.63}$$

it means D must have 1,3 as its elements and some extra number. Now

$$D = \{1, 2, 3, 4\} \tag{2.4.64}$$

means the extra member must be 3 or 4. Therefore:

$$D = \{1, 2, 3\} \quad \text{or} \quad D = \{1, 2, 4\} \tag{2.4.65}$$

Example 13

Problem: Show that the set D:

$$D = \{x|x \quad \text{is a real number} \quad x^2 \quad \text{and} \quad 2x = 6\} \tag{2.4.66}$$

is an empty set.

Solution: If

$$x \in D \tag{2.4.67}$$

then

$$x^2 = 16 \rightarrow x = 4, -4 \tag{2.4.68}$$

Also

$$2x = 6 \rightarrow x = 3 \tag{2.4.69}$$

But $x = 4, -4$ from the other condition. So D has no elements and is therefore $\emptyset$.

2.5 Power set

The set of all subsets of a given set D is called the *power set* of D and is denoted by P(D). The name power set is motivated by the fact that 'If D has n elements then its power set P(D) contains exactly 2^n elements.

Example 14

Problem: Lets define:

$$D = \{1, 2\} \tag{2.5.1}$$

Find P(D)

Solution: $\emptyset$ is a subset of D, D is a subset of D. So are $\{1\}$ and $\{2\}$ These are all subsets of D, therefore:

$$P(D) = \{\emptyset, \{1\}, \{2\}, D\} \tag{2.5.2}$$

Note that P(D) has 2^2 elements.

Example 15

Problem: Let

$$D = \{1, 2, 3\} \tag{2.5.3}$$

Find P(D).

Solution:

$$P(D) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, D\} \tag{2.5.4}$$

Once again P(D) has 2^3 elements.

Example 16

Problem: Two finite sets have m and n elements. The number of subsets of the first set is 30 more than the number of subsets of the second. Find m and n.

Solution: Suppose the first set has m elements, so the number of subsets is 2^m. Similarly if the second set has n elements, it will have 2^n subsets. So we know that:

$$2^m - 2^n = 30 \tag{2.5.5}$$

The only solution is that m = 5 and n = 1.

Example 17

Problem: Let K be a subset of D such that:

$$P(D : K) = \{X \in P(D) | K \subseteq X\} \tag{2.5.6}$$

If

$$K = \{1,2\} \tag{2.5.7}$$

$$D = \{1,2,3,4,5\} \tag{2.5.8}$$

list all the members of P(D:K).

Solution:

$$P(D) = \{\emptyset, 1, 2, 3, ...\} \quad 2^5 \text{ possibilities} \tag{2.5.9}$$

and K is a subset of these elements. Therefore:

$$\begin{aligned}
K &\subseteq \{1,2\} \\
&\subseteq \{1,2,3\} \\
&\subseteq \{1,2,3,4\} \\
&\subseteq \{1,2,3,4,5\} \\
&\subseteq \{1,2,4\} \\
&\subseteq \{1,2,5\} \\
&\subseteq \{1,2,3,5\} \\
&\subseteq \{1,2,4,5\}
\end{aligned} \tag{2.5.10}$$

These give all the elements of P(D:K).

2.6 Operation with sets

The reader should be familiar with the operators of addition and multiplication in Arithmetic. Given any two numbers, the operations of addition and multiplication associate another number called sum or product of the two numbers respectively. These are two of the most common operations. Fundamentally, these are just definitions and one can define any kind of operation. For example I may define an operation '*' as:

$$* = \frac{2 \times \text{number}}{2^{number}} \tag{2.6.1}$$

Such that:

$$4* = \frac{2 \times 4}{2^4} = \frac{1}{2} \tag{2.6.2}$$

And an infinite number of other operations can be define. The major use of operators is seen in quantum mechanics, where every physical observable as a *Hermitian* operator associated to it. The operator is applied to the wave-function of the system to yield an answer.

In the chapter on logic, the connectives $\wedge, \vee, \sim, \Rightarrow, \Leftrightarrow$ were used to associate with any two given statements a new statement which is called a compound statement. In this section we will define three operators namely, union, intersection and complementation and these will be analogous to the operations of addition, multiplication and subtraction of numbers respectively.

2.6.1 Union

The union of any two sets D and K is the set of all those elements, x such that x belongs to at least one of the sets D and K. It is denoted by:

$$D \cup K \tag{2.6.3}$$

We can also define this operation using logic. If the bi-conditional statement:

$$(x \in C) \Leftrightarrow (x \in D) \vee (x \in K) \tag{2.6.4}$$

In other words:

$$(x \in D \cup K) \equiv (x \in D) \vee (x \in K) \tag{2.6.5}$$

Example 18

Problem: If:

$$D = \{1, 2, 3\} \tag{2.6.6}$$

and

$$K = \{3, 4\} \tag{2.6.7}$$

Find the union of the two sets.

Solution:

$$D \cup K = \{1, 2, 3, 4\} \tag{2.6.8}$$

Example 19

Problem: Prove that for any sets D and K:

$$D \subseteq D \cup K \tag{2.6.9}$$

Solution:

$$x \in D \tag{2.6.10}$$

means:

$$x \in D \cup K \tag{2.6.11}$$

by definition. So

$$K \subseteq D \cup K \tag{2.6.12}$$

Or in terms of logic, we want to prove the conditional statement:

$$(x \in D) \Rightarrow (x \in D \cup K) \tag{2.6.13}$$

is true.

But this statement is false if and only if:

$$x \in D \tag{2.6.14}$$

is true and

$$x \in D \cup K \tag{2.6.15}$$

is false. Such a situation cannot occur, for

$$x \in D \tag{2.6.16}$$

is true which implies that:

$$(X \in D) \vee (x \in K) \tag{2.6.17}$$

is true. Therefore:

$$(x \in D) \vee (x \in K) \tag{2.6.18}$$

is true and:

$$x \in D \cup K \tag{2.6.19}$$

is false. It means:

$$(x \in D) \vee (x \in K) \Rightarrow (x \in D \cup K) \tag{2.6.20}$$

is false. This is a contradiction as:

$$x \in D \cup K \tag{2.6.21}$$

means x is an element of either one of D or K sets.

Example 20

Problem: If:

$$D \subseteq K \tag{2.6.22}$$

then

$$D \cup K = k \tag{2.6.23}$$

and conversely, if:

$$D \cup K = K \tag{2.6.24}$$

then

$$D \subseteq K \tag{2.6.25}$$

Solution: Suppose

$$D \subseteq K \tag{2.6.26}$$

Let:

$$x \in D \cup K \tag{2.6.27}$$

Then

$$x \in D \tag{2.6.28}$$

or in any case:

$$x \in D \cup K \tag{2.6.29}$$

means:

$$x \in K \tag{2.6.30}$$

So:

$$D \cup K \subseteq K \tag{2.6.31}$$

We have already proved:

$$D \equiv D \cup K \tag{2.6.32}$$

which means:

$$x \in K \tag{2.6.33}$$

so

$$D \subseteq K \tag{2.6.34}$$

In terms of logic; suppose $D \subseteq K$. We want to show that the bi-conditional statment:

$$(x \in K) \Leftrightarrow (xinD) \vee (x \in K) \tag{2.6.35}$$

is true for every x. But this statement is false if and only if $(x \in K)$ is flase and $(x \in D)$ is true. But this is not possible as:

$$D \subseteq K \tag{2.6.36}$$

which means that all the elements in D are also in K. This proves that:

$$D \cup K = K \tag{2.6.37}$$

Now we want to show that the conditional statement:

$$(x \in D) \Rightarrow (x \in K) \tag{2.6.38}$$

is true for ever x. This is false if and only if

$$(x \in D) \tag{2.6.39}$$

is true and:

$$(x \in K) \tag{2.6.40}$$

is false. Now since Eq 2.6.39 is true, it means that Eq 2.6.38 is true. Therefore:

$$(x \in D) \vee (x \in K) \rightarrow (x \in K) \tag{2.6.41}$$

is false. This is impossible as:

$$K = D \cup K \tag{2.6.42}$$

This proves that $D \subseteq K$.

Example 21

Problem: Prove that if $D \subseteq C$ and $K \subseteq C$ then $(D \cup K) \subseteq C$.

Solution: We want to show:

$$(x \in D \cup K) \Rightarrow (x \in C) \tag{2.6.43}$$

is true for every x. This is equivalent to saying that:

$$x \in D \cup K \tag{2.6.44}$$

is true and

$$(x \in C) \tag{2.6.45}$$

is false cannot occur together. Suppose Eq 2.6.44 is true, then:

$$(x \in D) \vee (x \in K) \tag{2.6.46}$$

is true. This means

$$x \in D \tag{2.6.47}$$

is true or:

$$x \in K \tag{2.6.48}$$

is true as $D \subseteq C$. In any case $x \in C$ should also be true. This proves our assertion.

Another way to do this; let:

$$x \in D \cup K \tag{2.6.49}$$

This means $x \in D$ or $x \in K$ or $x \in D$ and K. If:

$$x \in D \tag{2.6.50}$$

then

$$x \in C \tag{2.6.51}$$

as $D \subseteq C$. If $x \in K$, then $x \in C$ as $K \subseteq C$. In any case, $x \in C$. So:

$$x \in D \cup K \tag{2.6.52}$$

means $x \in C$, so we have proved that:

$$D \cup K \subseteq C \tag{2.6.53}$$

2.6.2 Intersection

The intersection of two sets D and K is the set of all those elements x such that x belongs to both D and K and is denoted by:

$$D \cap K = \emptyset \tag{2.6.54}$$

i.e, they do not intersect, then D and K are said to be disjoint. Logically speaking, if the bi-conditional statement:

$$(x \in C) \Leftrightarrow (x \in D) \wedge (x \in K) \tag{2.6.55}$$

is true for all x, then:

$$C = D \cap K \tag{2.6.56}$$

In other words:

$$(x \in D \cap K) \equiv (x \in D) \cap (x \in K) \tag{2.6.57}$$

Example 22

Problem 1: If:

$$D = \{1, 2, 3, 4\}, \quad K = \{1, 2\} \tag{2.6.58}$$

What is $D \cap K$?

Solution 1:

$$D \cap K = \{1, 2\} \tag{2.6.59}$$

Problem 2: If

$$D = \{1, 2, 3, \quad K = \{4, 5\} \tag{2.6.60}$$

What is $D \cap K$?

Solution 2:

$$D \cap K = \emptyset \tag{2.6.61}$$

Example 23

Problem 1: Prove

$$D \cap K \subseteq D \tag{2.6.62}$$

Solution 1: Let

$$x \in D \cap K \tag{2.6.63}$$

Then by definition:

$$x \in D \tag{2.6.64}$$

and

$$x \in K \tag{2.6.65}$$

So:

$$D \cap K \subseteq D \tag{2.6.66}$$

and

$$D \cap K \subseteq K \tag{2.6.67}$$

In logical terms; we want to show that:

$$x \in D \cap K \Rightarrow x \in D \tag{2.6.68}$$

is true for all x. We have to only consider the case when:

$$x \in D \cap K \tag{2.6.69}$$

is true and $x \in D$ is false. Now $x \in D$ is false shall mean:

$$x \in D \cap (x \in K) \tag{2.6.70}$$

is false so:

$$(x \in D \cap K) \Rightarrow (x \in D) \cap (x \in K) \tag{2.6.71}$$

is also false which is impossible by the definition of $(D \cap K)$. This proves the result.

Problem 2: Prove:

$$D \cap K \subseteq K \tag{2.6.72}$$

Solution 2: We want to show that:

$$x \in D \cap K \Rightarrow x \in K \tag{2.6.73}$$

is true for all x. The only doubtful case is when:

$$x \in D \cap K \tag{2.6.74}$$

is true and:

$$x \in K \tag{2.6.75}$$

is false. But this is not possible by the definition of $D \cap K$.

Example 24

Problem: Prove that if:

$$D \subseteq K \ \text{and} D \subseteq C \tag{2.6.76}$$

Then:

$$D \subseteq (K \cap C) \tag{2.6.77}$$

Solution: Let:

$$x \in D \tag{2.6.78}$$

Then:

$$x \in K \tag{2.6.79}$$

and

$$x \in C \tag{2.6.80}$$

So we see that:

$$x \in D \cap K \tag{2.6.81}$$

This proves that:

$$D \subseteq K \cap C \tag{2.6.82}$$

In logical terms we want to show that:

$$(x \in D) \Rightarrow (x \in K \cap C) \tag{2.6.83}$$

is true for all x. The only doubtful case is when $x \in C$ is true and $(x \in D \cap C)$ is false. Now $(x \in D)$ is true means $(x \in K)$ is also true as $D \subseteq K$. This means:

$$(x \in K) \cap (x \in C) \tag{2.6.84}$$

is true and so $(x \in K \in C)$ is true. This proves the result.

Example 25

Problem: Prove:

$$D \cup K = D \cap K \quad \text{if and only if} \quad D = K \tag{2.6.85}$$

Solution: Suppose

$$D \cup K = D \cap K \tag{2.6.86}$$

Lets define:

$$x \in D \tag{2.6.87}$$

Then

$$x \in D \cup K \tag{2.6.88}$$

and therefore:

$$x \in D \cap K \tag{2.6.89}$$

Therefore $x \in K$. This proves that:

$$D \subseteq K \tag{2.6.90}$$

and so:

$$x \in D \cap K \tag{2.6.91}$$

Therefore, $x \in K$. This proves $D \subseteq K$. Similarly $K \subseteq D$ and so $D = K$.

Now lets do it logically and here we introduce a new law, called the *Absorption law* defined as:

$$d \cap (d \cup k) \equiv d \tag{2.6.92}$$

$$d \cup (d \cap k) \equiv d \tag{2.6.93}$$

where d and k represent statements here. Now suppose:

$$D \cup K = D \cap K \tag{2.6.94}$$

Then we have:

$$\begin{aligned}
(x \in D) &\equiv (x \in D) \cap ((x \in D) \vee (x \in K)) \\
&\equiv (x \in D) \wedge ((x \in D \cup K)) \\
&\equiv (x \in D) \wedge (x \in D \cap K) \\
&\equiv ((x \in D) \wedge (x \in D)) \wedge (x \in K) \\
&\equiv (x \in D) \wedge (x \in K) \\
&\equiv (x \in D \cap K) \\
&\equiv (x \in D \cup K) \\
&\equiv (x \in K) \vee (x \in D) \\
&\equiv (x \in K) \vee ((x \in D) \cup (x \in D)) \\
&\equiv (x \in K) \vee ((x \in K \cup D)) \\
&\equiv (x \in K) \vee (x \in D \wedge K) \\
&\equiv (x \in K) \vee ((x \in D) \wedge (x \in K)) \\
&\equiv (x \in K) \vee ((x \in D) \wedge (x \in K)) \\
&\equiv ((x \in K) \vee (x \in D)) \wedge (x \in K) \\
&\equiv x \in K \qquad (2.6.95)
\end{aligned}$$

This proves that $D = K$. Which means that:

$$\begin{aligned}
(x \in D \cup K) &\equiv (x \in D) \cup (x \in K) \\
&\equiv (x \in K) \cup (x \in K) \\
&\equiv (x \in K) \\
&\equiv (x \in K) \cap (x \in K) \\
&\equiv (x \in D) \cap (x \in K) \\
&\equiv (x in D \cap K) \qquad (2.6.96)
\end{aligned}$$

Example 26

Problem: If

$$D \cup K = D \cup K \tag{2.6.97}$$

and

$$D \cap K = D \cap C \tag{2.6.98}$$

Show that $K = C$.

Solution: Let k $\in K.Then$

$$k \in D \cup K \Rightarrow k \in D \cup C \tag{2.6.99}$$

So, $k \in D$ or $k \in C$. If $k \in D$, then:

$$k \in D \cap K \Rightarrow k \in D \cap C \Rightarrow k \in C \tag{2.6.100}$$

Therefore, $K \subseteq C$. Similarly $C \subseteq K$. Thus $K = C$.

Example 27

Problem: Let

$$D = \{2n| \quad \text{n is an integer}\} \tag{2.6.101}$$

$$K = \{2m| \quad \text{m is an integer}\} \tag{2.6.102}$$

Show that:

$$\{D \cap L\} = \{6r| \quad \text{r is an integer}\} \tag{2.6.103}$$

Solution:

$$x \in D \cap K \Rightarrow x \in D \tag{2.6.104}$$

and

$$x \in K \Rightarrow 2 \tag{2.6.105}$$

divides x and 3 divides $x \Rightarrow$ 6 divides $x \Rightarrow x$ is an integer multiple of $6 \Rightarrow x \in \{6r|r$ is an integer. Conversely let $x \Rightarrow 6r$. Then 2 divides x and 3 divides $x \Rightarrow x$ is a multiple of 2 as well as $3 \Rightarrow x \in D \cap K$.

Note that a set is always a subset of a fixed set U, this fixed set U will be called the *universal* set.

2.6.3 Complements

If D and K are two sets, then complement of K relative to D is defined as the set of all these elements, $x \in D$ such that $x \notin K$ and is denoted by $D - K$. Logically speaking, if for a set C, the bi-conditional statement:

$$(x \in C) \Leftrightarrow (x \in D) \cap (x \notin K) \tag{2.6.106}$$

is true for all x, then:

$$C = D - K \tag{2.6.107}$$

In other words, if:

$$(x \in C) \equiv (x \in D) \wedge (x \notin K) \tag{2.6.108}$$

then C is called the complement of K and D.

It is worth noting that $D - K$ is a subset of D. Whenever we say the complement of K we mean the complement of K relative to the universal set, U. In such a case, we denote complement of K by K':

$$K' = U - K \tag{2.6.109}$$

Example 28

Problem: If:

$$D = \{1, 2, 3, 4\} \tag{2.6.110}$$

$$K = \{3, 4, 5\} \tag{2.6.111}$$

then what is $D - K$?

Solution

$$D - K = \{1, 2\} \tag{2.6.112}$$

Example 29

Problem: Show that:

$$D - K = D \cap K' \tag{2.6.113}$$

Solution: Let:

$$x \in D - K \tag{2.6.114}$$

This means $x \in D$ and $x \notin K$. By the definition of the universal set:

$$D - K \subseteq U \tag{2.6.115}$$

So $x \in U$. Therefore $x \in U.x \notin K$, implies $x \in K$. This proves:

$$D - K \subseteq D \cap K \tag{2.6.116}$$

Now $x \in K'$ implies $x \in K$. So:

$$x \in D - K \tag{2.6.117}$$

This proves:

$$D \cap K' \subseteq D - K \tag{2.6.118}$$

Therefore:

$$D - K = D \cap K' \tag{2.6.119}$$

In logical terms:

$$\begin{aligned}(x \in D - K) &\equiv (x \equiv D) \wedge (x \notin K)\\ &\equiv (x \in D \wedge U) \wedge (x \in K) \quad \text{as} \quad D \wedge U = D\\ &\equiv ((x \in D) \wedge (x \in U)) \wedge (x \notin K)\\ &\equiv (x \in D) \wedge ((x \in U) \wedge (x \notin K))\\ &\equiv ((x \in D) \wedge (x \in K'))\end{aligned} \tag{2.6.120}$$

This proves that:

$$D - K = D \cap K' \tag{2.6.121}$$

Example 30

Problem: Show that:

$$D \subseteq K \quad \text{if and only if} \quad D' \subseteq K' \tag{2.6.122}$$

Solution: Suppose that:

$$D \subseteq K \tag{2.6.123}$$

Let:

$$x \subseteq K' \tag{2.6.124}$$

Then $x \subset U$ and $x \notin K$. Now $x \notin K$ implies xD (as $D \subset K$). Therefore $x \in U$ and $x \notin D$ means $x \in D'$. This proves that:

$$K' \subseteq D' \tag{2.6.125}$$

Conversely, let:

$$K' \subseteq D' \tag{2.6.126}$$

Let:

$$x \in D \tag{2.6.127}$$

Then $x \in D$. Now $x \notin D'$ implies that $x \notin K'$ (as $K' \subseteq D'$). This means $x \in K$. So $D \subseteq K$.

In terms of logic:

$$\begin{aligned}(x \in D) &\Rightarrow (x \in K)\\ &\equiv \sim (x \in K) \Rightarrow \sim (x \in D) \quad \text{(Contra-positive law in logic)}\\ &\equiv (x \notin K) \Rightarrow (x \notin D)\\ &\equiv (x \in K') \Rightarrow (x \in D')\end{aligned} \tag{2.6.128}$$

Suppose $D \subseteq K$. Then:

$$(x \in D) \Rightarrow (x \in K) \tag{2.6.129}$$

is true for all x. We saw above that:

$$(x \in D) \Rightarrow (x \in K) \tag{2.6.130}$$

is true for all x. This implies $D \subseteq K$.

2.7 Algebra of sets

The best way to go about this section is to list the important laws that sets follow.

2.7.1 Law of Idempotence

For any set D:

$$D \cup D = D \quad \text{and} \quad D \cap D = D \tag{2.7.1}$$

Idempotence just means an operation that returns a value identical to its arguments. The proof for the law above is obvious.

2.7.2 Commutative laws

For any sets D and K:

$$D \cup K = K \cup D \quad \text{and} \quad D \cap K = K \cap D \tag{2.7.2}$$

Proof is obvious.

2.7.3 Associative law

For any three sets D, K, C:

$$D \cup (K \cup C) = (D \cup K) \cup C \tag{2.7.3}$$

To prove this, we want to show that:

$$(x \in D \cup (K \cup C)) = ((x \in D) \cup (x \in K) \cup (x \in C)) \tag{2.7.4}$$

This follows from the associative law in logic. A similar result to this is also:

$$D \cap (K \cap C) = (D \cap K) \cap C \tag{2.7.5}$$

2.7.4 Distributive laws

For any three sets D, K, C:

$$D \cap (K \cup C) = (D \cap K) \cup (D \cup C) \tag{2.7.6}$$

To prove this, lets define:

$$x \in D \cap (K \cup C) \tag{2.7.7}$$

This implies:

$$x \in D \tag{2.7.8}$$

and

$$x \in K \cup C \tag{2.7.9}$$

Now, Eq 2.7.9 implies $x \in K$ or $x \in C$ or $x \in K \quad \text{and} \quad C$. If:

$$x \in K \tag{2.7.10}$$

then, $x \in D \cap K$. If $x \in C$ then:

$$x \in D \cap C \tag{2.7.11}$$

In any case:

$$x \in (D \cap K) \cup (D \cap C) \tag{2.7.12}$$

So,

$$D \cap (K \cup C) \subseteq (D \cap K) \cup (D \cap C) \tag{2.7.13}$$

Similarly:

$$(D \cap K) \cup (D \cap C) \subseteq D \cap (K \cup C) \tag{2.7.14}$$

This proves the Eq 2.7.6.

We can also use logic to prove it:

$$\begin{aligned} x \in (D \cap (K \cup C)) &\equiv ((x \in D) \wedge (x \in K \cup C)) \\ &\equiv ((x \in D) \wedge ((x \in K) \vee (x \in C))) \\ &\equiv ((x \in D) \wedge (x \in K)) \vee ((x \in D) \subset (x \in C)) \quad \text{(distributive law in logic)} \\ &\equiv (x \in (D \cap K)) \cup (x \in (D \cap C)) \\ &\equiv (x \in (D \cap K) \cup (D \cap C)) \end{aligned} \tag{2.7.15}$$

So:

$$D \wedge (K \cup C) = (D \cap K) \cup (D \cap C) \tag{2.7.16}$$

A similar expression can be derived:

$$D \cup (K \cap C) = (D \cup K) \cap (D \cup C) \tag{2.7.17}$$

2.7.5 De-Morgans laws

For any two sets D and K:

$$(D \cup K)' = D' \cap K' \tag{2.7.18}$$

To prove it, let:

$$x \in (D \cup K)' \tag{2.7.19}$$

This implies:

$$x \notin D \cup K \tag{2.7.20}$$

and:

$$x \in U \tag{2.7.21}$$

Now, $x \notin D \cup K$ implies that $x \notin D$ and $x \in U$ implies $x \in D'$ and $x \notin K$ and $x \in U$ implies $x \in K'$. Therefore $x \in D' \cap K'$ and so:

$$(D \cup K') \subseteq D' \cap K' \tag{2.7.22}$$

Similarly:

$$(D' \cap K') \subseteq (D \cup K)' \tag{2.7.23}$$

This completes the proof. An alternative proof using logic:

$$\begin{aligned}
x \in (D \cup K)' &\equiv \sim((x \in (D \cup K))) \\
&\equiv \sim((x \in D) \vee (x \in K)) \\
&\equiv \sim(x \in D) \wedge \sim(x \in K) \\
&\equiv (x \notin D) \wedge (x \notin K) \\
&\equiv (x \in D') \wedge (x \in K') \\
&\equiv (x \in D' \wedge K')
\end{aligned} \tag{2.7.24}$$

Therefore:

$$(D \cup K)' = D' \cap K' \tag{2.7.25}$$

A similar expression is:

$$(D \cap K)' = D' \cup K' \tag{2.7.26}$$

This also has a similar proof.

Example 31

Problem: Let D, K, C be any three sets. Prove:

$$D \cap (K - C) = (D \cap K) - (D \cap C) \tag{2.7.27}$$

Solution:

$$\begin{aligned}
(D \cap K) - (D \cap C) &= (D \cap K) \cap (D \cap C) \\
&= (D \cap K) \cap (D' \cup C') \quad \text{(De Morgans laws)} \\
&= ((D \cap K) \cap D') \cup ((D \cap K) \cap K') \quad \text{(Distributive law)} \\
&= ((D \cap D') \cap K) \cup ((D \cap K) \cap C') \quad \text{(Associative law)} \\
&= (\emptyset \cap K) \cup (D \cap (K \cap C')) \\
&= \emptyset \cup (D \cap (K \cap C')) \\
&= D \cap (K \cap C') \equiv D \cap (K - C)
\end{aligned} \tag{2.7.28}$$

Example 32

Problem: For any sets D and K, show that:

$$(D - K) \cup (K - D) = (D \cup K) - (D \cap K) \tag{2.7.29}$$

Solution:

$$\begin{aligned}
(D - K) \cup (K - D) &= (D \cup K) \cap (D \cap K)' \\
&= (D \cup K) \cap (D' \cup K') \quad \text{(De Morgans laws)} \\
&= ((D \cup K) \cap D') \cup ((D \cup K) \cap K') \quad \text{(Distributive law)} \\
&= ((D \cap D') \cup (K \cap D')) \cup ((D \cap K') \cup (K \cap K')) \\
&= (\emptyset \cup (K \cap D')) \cup ((D \cap K') \cup \emptyset) \\
&= (K \cap D') \cup (D \cap K') \\
&= (K - D) \cup (D - K) \\
&= (D - K) \cup (K - D) \quad \text{(Commutative law)} \qquad (2.7.30)
\end{aligned}$$

2.8 VENN Diagrams

Now that we have discussed the concept of operations on sets, we can introduce a set of diagrams, called *Venn diagrams* that can be used to illustrate the various set operators. We shall represent the universal set by the points in and on a rectangle and subset $D, K..$ by points in and on the circles or ellipses down inside the rectangle.

As an example consider:

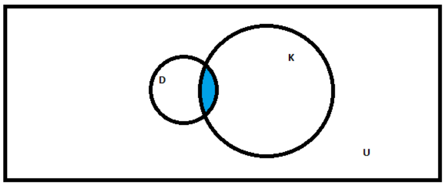

Figure 14: Venn diagram representing $D \cap K$ in the shaded region

Here the shaded region represents $D \cap K$. Here are a few more examples:

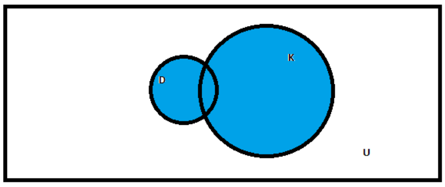

Figure 15: Venn diagram representing $D \cup K$ in the shaded region

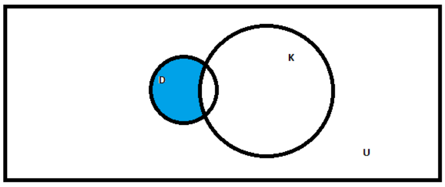

Figure 16: Venn diagram representing $D - K$ in the shaded region

Now consider a different type of Venn diagram. This shows the region that is not included in the set, in other words it represents the region corresponding to D':

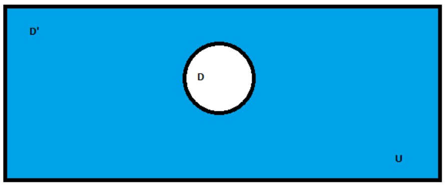

Figure 17: Venn diagram representing D' in the shaded region

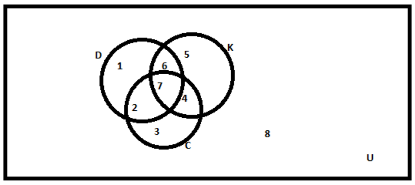

Figure 18: Universal set divided into 8 subsets

Example 33

Problem: Prove that:

$$D \cup (K \cap C) = (D \cup K) \cap (D \cup C) \tag{2.8.1}$$

using Venn diagrams.

Solution: $K \cap C$ is represented by regions 4 and 7 in Fig 18. Therefore $D \cup (K \cap C)$ is represented by $1, 2, 4, 6, 7$. $D \cup K$ is represented by 6,7,1,2,5,4. $D \cap C$ is represented by 2,7,1,6,4,3.

Therefore:

$$(D \cup K) \cap (D \cup C) = 1, 2, 4, 6, 7 \tag{2.8.2}$$

Example 34

Problem: Using Venn diagrams show that:

$$D - (K \cup C) = (D - K) \cap (D - C) \tag{2.8.3}$$

Solution: $K \cup C$ has regions 2,3,4,5,6,7 D has regions 1,2,6,7

Therefore $D - (K \cup C)$ means regions in D and not in $(K \cup C)$. The only region in D that is not in $K \cup C$ is 1. $D - K$ means regions in D and not in K; 1,2. $D - C$ gas regions 1,6.
Therefore:

$$(D - K) \cap (D - C) = 1 \tag{2.8.4}$$

This proves the result.

Example 35

Problem: Using Venn diagrams show that for any two sets D and K:

$$(D \cap K)' = D' \cup K' \tag{2.8.5}$$

Solution: First lets draw the Venn diagram:

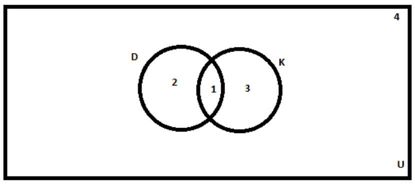

Figure 19: Universal set divided into 8 subsets

In this diagram, $D \cap K$ represents region 1. Therefore $(D \cap K)'$ represents region 2,3,4. D' represents regions 3,4 K' represents regions 2,4 Therefore $D' \cup K' = 2, 3, 4$. Which completes the proof.

Example 36

Problem: Use Venn diagrams to show that for any sets D and K:

$$D \cup K = D \cup (K - D) \tag{2.8.6}$$

Solution: In the diagram in example 35, $D \cup K$ represents regions 1,2,3. $D \cup K$ represents regions 1,2,3. $K - D$ represents region 3. $D \cup (K - D)$ represents 1,2,3. This proves the equivalence.

2.9 Applications

If D us a finite set, then we shall denote the number of elements in D by:

$$n(D) = \text{Number of elements in } D \tag{2.9.1}$$

If D and K are two finite sets, then it is very clear from the Venn diagram of $D - K$ that:

$$n(D - K) = n(D) - n(K \cap D) \tag{2.9.2}$$

Suppose D and K are two finite sets such that:

$$D \cap K = \emptyset \tag{2.9.3}$$

Then it is obvious (at least it is to me) that the number of elements in $D \cup K$ is the sum of the number of elements in D and the number of elements in K:

$$n(D \cup K) = D \cup (K - D) \tag{2.9.4}$$

Here:

$$D \cap (K - D) = \emptyset \tag{2.9.5}$$

Therefore:

$$\begin{aligned} n(D \cup K) &= n(D) + n(K - D) \\ &= n(D) + n(K) - n(D \cap K) \end{aligned} \tag{2.9.6}$$

Note that from the definition of the empty set it follows that $n(\emptyset) = 0/$ So we have proved that, 'If D and K are finite sets'. then:

$$n(D \cup K) = n(D) + n(K) - n(D \cap K) \tag{2.9.7}$$

Similarly, if D, K, C are three finite sets, then:

$$\begin{aligned} n(D \cup K \cup C) &= n(D \cup K) + n(C) - n((D \cup K) \cap C) \\ &= n(D) + n(K) - n(D \cap K) + n(C) - n((D \cup K) \cap C) \\ &= n(D) + n(K) + n(C) - n(D \cap K) - n(D \cap C) - n((D \cap C) \cup (K \cap C)) \\ &= n(D) + n(K) + n(C) - n(D \cap K) - (n(D \cap C) + n(K \cap C) - n((D \cap C) \cap (K \cap C))) \\ &= n(D) + n(K) + n(C) - n(D \cap C) - n(K \cap C) + n(D \cap K \cap C) \end{aligned} \tag{2.9.8}$$

Example 37

Problem: In a recent survey of 400 students in a school , 100 were listed as smokers and 150 used to chew tobacco, 75 were listed as both smokers and tobacco chewers. Find out how many students are neither smokers nor tobacco chewers.

Solution: Well, firstly one might think that there is simply no need to apply the rules of set theory here as the answer is quite obvious. However, starting to apply set theory to simple problems will help tackle more challenging problems, whose answers will not be so obvious.

Let U be the set of students being questioned. Let D be the set of students who smoke and K be the set of students who chew tobacco. Then:

$$n(U) = 400 \tag{2.9.9}$$

$$n(D) = 100 \tag{2.9.10}$$

$$n(K) = 150 \tag{2.9.11}$$

$$n(D \cap K) = 75 \tag{2.9.12}$$

We want to find:

$$n(D' \cap K') \tag{2.9.13}$$

Now:

$$D' \cap K' = (D \cup K)' = U - (D \cup K) \tag{2.9.14}$$

Therefore:

$$\begin{aligned} n(D' \cap K') &= n(U - (D \cup K)) \\ &= n(U) - n((D \cup K) \cap U) \\ &= n(U) - n(D \cup K) \\ &= n(U) - n(D) - n(K) + n(D \cap K) \\ &= 400 - 100 - 150 + 75 = 225 \end{aligned} \tag{2.9.15}$$

So there are 225 students who do not smoke or chew tobacco.

Example 38

Problem: Out of 500 car owners investigated, 400 owned BMW cars and 200 owned Audi cars; 50 owned both Audi and BMW cars. Is this data correct?

Solution: Let U be the set of the car owners who are involved in the investigation. Let D be the set of these people who own BMW cars and K be the set of people who won Audi cars. Then $D \cap K$ represents the set of people who own both BMW and Audi cars:

$$n(U) = 500 \tag{2.9.16}$$

$$n(D) = 400 \tag{2.9.17}$$

$$n(K) = 200 \tag{2.9.18}$$

$$n(D \cap K) = 50 \tag{2.9.19}$$

Therefore:

$$\begin{aligned} n(D \cup K) &= n(D) + n(K) - n(D \cap K) \\ &= 400 + 200 - 50 = 550 \end{aligned} \tag{2.9.20}$$

This shows that the data is not correct as the sum is greater than the total number of cars investigated.

Example 39

Problem: In a certain government office there are 400 employees; there are 150 men, 276 university graduate students, 212 married people, 94 male university graduate students, 151 married university graduates, 119 married men, 72 married male university graduates. Find the number of single women who are not university graduates.

Solution: Let:

$$\begin{aligned} U &= \text{Set of employees} \\ D &= \text{Set of men} \\ K &= \text{Set of married people} \\ C &= \text{Set of university graduates} \end{aligned}$$

Then:

$$\begin{aligned} D \cap K &= \text{Set of married men} \\ D \cap C &= \text{Set of male university graduate students} \\ K \cap C &= \text{Set of married university graduate students} \\ D \cap K \cap C &= \text{Set of married university male university graduate students} \end{aligned}$$

Now $n(U) = 400, n(D) = 150, n(K) = 212, n(C) = 276, n(D \cap K) = 119, n(D \cap C) = 94, n(K \cap C) = 151, n(D \cap K \cap C) = 72$. We want to find:

$$n(D' \cap K' \cap C') \tag{2.9.21}$$

Now:

$$\begin{aligned} (D' \cap K' \cap C') &= (D \cup K \cup C)' \\ &= U - (D \cup K \cup C) \end{aligned}$$

Therefore:

$$\begin{aligned} n(D' \cap K' \cap C') &= n(U) - n((D \cup K \cup C) \cap U) \\ &= n(U) - n(D \cup K \cup C) \\ &= n(U) - (n(D) + n(K) + n(C) - n(D \cap K) - n(D \cap C)) \\ &= n(K \cap C) + n(D \cap K \cap C) \\ &= 764 - 710 = 54 \end{aligned} \tag{2.9.22}$$

So the number of single women who are not university graduates is 54.

Example 40

Problem: A market researcher conducted a survey of 1000 consumers and reported that 720 consumers liked product A and 450 consumers like product B. What is the least number that must have like both products?

Solution: Lets define:

$$\begin{aligned} U &= \text{Set of consumers being questioned} \\ D &= \text{Set of consumers who liked A} \\ K &= \text{Set of consumers who liked B} \end{aligned}$$

Then:

$$D \cap K = \text{Set of consumers who like both products}$$

Now; $n(U) = 100, n(D) = 720, n(K) = 450$. Therefore:

$$\begin{aligned} n(D \cup K) &= n(D) + n(K) - n(D \cap K) \\ &= 1170 - n(D \cap K) \end{aligned} \tag{2.9.23}$$

Now $n(D \cap K)$ is least when $n(D \cup K)$ is maximum. But $D \cup K \subseteq U$ implies that:

$$n(D \cap K) \leq n(U) \tag{2.9.24}$$

This means the maximum value of $n(D \cup K)$ is 1000. So the least value of $n(D \cap K)$ is 170. Therefore there must have been atleast 170 people who liked both products.

Example 41

Problem: Out of 1000 students who appeared for C.A intermediate exam, 750 failed in maths, 500 failed in accounts and 600 failed in costing, 450 failed in both maths and accounting, 400 failed in both maths and costing, 150 failed in both accounts and counting. There were 75 students who failed all the subjects. Prove that the above data is incorrect.

Solution: Lets define:

$$\begin{aligned} U &= \text{Set of students that appeared in the exam} \\ D &= \text{Set of students who failed in maths} \\ K &= \text{Set of students who failed in accounts} \\ C &= \text{Set of students who failed in costing} \end{aligned}$$

Then:

$$\begin{aligned} D \cap K &= \text{Set of students who failed maths and accounts} \\ K \cap C &= \text{Set of students who failed in accounts and costing} \\ D \cap C &= \text{Set of students who failed in maths and costing} \\ D \cap K \cap C &= \text{Set of students who failed in all three subjects} \end{aligned}$$

Now $n(U) = 1000, n(D) = 750, n(K) = 600, n(C) = 600, n(D \cap K) = 450, n(K \cap C) = 150, n(D \cap C) = 400, n(D \cap K \cap C) = 75$.

Therefore:

$$n(D \cup K \cup C) = 750 + 600 + 600 - 450 - 150 - 400 + 75 = 1025 \qquad (2.9.25)$$

This exceeds the total number of students who appeared in the exam, hence the data is not correct.

Example 42

Problem: In a survey of 100 families, the number that read recent issues of a certain monthly magazine were found to be:

$$\begin{aligned} \text{Only September} &= 15 \\ \text{September but not August} &= 23 \\ \text{September and July} &= 8 \\ \text{September} &= 26 \\ \text{July} &= 48 \\ \text{July and August} &= 8 \\ \text{None of the three months} &= 24 \end{aligned}$$

Find: How many read the August issue? How many read two consecutive issues? How many read the July issue, if and only if they did not read the August issue? How many read the September and August issue but not the July issue.

Solution: Lets define:

$$\begin{aligned} D &= \text{Set of families that read September issue} \\ K &= \text{Set of families that read August issue} \\ C &= \text{Set of families who read the July issue} \end{aligned}$$

Then:

$$\begin{aligned} D - K &= \text{Set of families that read September issue but not the August issue} \\ D \cap C &= \text{Set of those families that read both Sept and July issues} \\ D \cap K &= \text{Set of those families that read both September and August issues} \\ D' \cap K' \cap C' &= \text{Set of those families that read none} \\ D - (K \cup C) &= \text{Set of families that read September only} \end{aligned}$$

Now; $n(D) = 26, n(C) = 48, n(D - K) = 23, n(D \cap C) = 8, n(K \cap C) = 8, n(D' \cap K' \cap C') = 24, n(D - (K \cup C)) = 18$. Now lets do:

$$\begin{aligned} n(D-K) &= n(D)-n(D\cap K) \\ 28 &= 26-n(D\cap K) \end{aligned} \tag{2.9.26}$$

Therefore $n(D \cap K) = 3$. So three families read September and August issues.

Again:

$$n(D-(K\cup C)) = n(D) - n(D\cap(K\cup C)) \tag{2.9.27}$$

So:

$$\begin{aligned} 18 &= 26 - n((D\cap K)\cup(D\cap C)) \\ &= 26 - n(D\cap K) - n(D\cap C) + n(D\cap K\cap C) \\ &= 26 - 3 - 8 + n(D\cap K\cap C) \end{aligned} \tag{2.9.28}$$

Therefore:

$$n(D\cap K\cap C) = 3 \tag{2.9.29}$$

So three families read all three issues.

Also:

$$D'\cap K'\cap C' = (D\cup K\cup C)' = U - (D\cup K\cup C) \tag{2.9.30}$$

where U is the set of families being questioned, $n(U) = 100$:

$$\begin{aligned} n(D'\cap K'\cap C') &= n(U) - n(D\cup K\cup C) \\ 24 &= 100 - n(D\cup K\cup C) \end{aligned} \tag{2.9.31}$$

Therefore $n(D\cup K\cup C) = 76$. Now:

$$n(D\cup K\cup C) = n(D)+n(K)+n(C)-n(D\cap K)-n(D\cap C)-n(K\cap C)+n(D\cap K\cap C) \tag{2.9.32}$$

Implies that:

$$76 = 26 + n(K) + 48 - 3 - 8 - 8 + 3 \tag{2.9.33}$$

Therefore:

$$n(K) = 18 \tag{2.9.34}$$

So 18 families read the August issue. Now:

$(D\cap K)\cup(K\cap C) =$ Set of families who reed two consecutive issues

So;

$$n((D \cap K) \cup (K \cap C)) = n(D \cap K) + n(K \cap C) - n(D \cap K \cap C) = 3 = 8 - 3 = 8 \quad (2.9.35)$$

Again;

$$C - K = \text{Set of families that read the July issue and not the August issue}$$

Then:

$$n(C - K) = n(C) - n(K \cap C) = 48 - 8 = 40 \quad (2.9.36)$$

Now;

$$(D \cap K) - C = \text{Set of those families that read the September and August issue but not July}$$

So;

$$n((D \cap K) - C) = n(D \cap K) - n(D \cap K \cap C) = 3 - 3 = 0 \quad (2.9.37)$$

Therefore:

$$(D \cap K) - C = \emptyset \quad (2.9.38)$$

So there are no families that read both September and August issues but not the July issue.

Example 43

Problem: A factory inspector examined the defects in dimension, finish and hardness of an item. After examining 100 items, he gave the following report: All three defects were in 5 items, defects in hardness and finish were in 10 items, defects in dimension and finish were in 8 items, defects in dimension and hardness were in 20 items, defects in finish were in 20 items, defects in hardness only were in 23, defects in dimension were in 50 items.
After this report the inspector was fined. Why?

Solution: Suppose:

$$H = \text{Set of items which have defects in hardness}$$

$$F = \text{Set of items with defect in finish}$$

$$D = \text{Set of items with defects in dimension}$$

Then:

$$\begin{aligned}
n(H \cap F \cap D) &= 5 \\
n(H \cap F) &= 10 \\
n(D \cap H) &= 20 \\
n(F) &= 30 \\
n(H) &= 23 \\
n(D) &= 50
\end{aligned}$$

So:

$$n(H \cup F \cup D) = 30 + 23 + 50 - 20 - 10 - 8 + 5 = 70 \tag{2.9.39}$$

Now:

$$n(D \cup F) = n(D) + n(F) - n(D \cap F) = 50 + 30 - 8 = 72 \tag{2.9.40}$$

But $D \cup F$ is a subset of $D \cup F \cup H$:

$$D \cup \subseteq D \cup F \cup H \tag{2.9.41}$$

Therefore we have:

$$n(D \cup F) \leq n(D \cup D \cup H) \Rightarrow 72 \leq 70 \tag{2.9.42}$$

Therefore the inspector must be lying and hence he was fined.

Example 44

Problem: In a survey of 100 families, the number that read the most recent issue of various magazines were found to be as follows:

Readers digest	=	28
Science today	=	30
Readers digest and science today	=	8
Caravan	=	42
Readers digest and caravan	=	10
Science today and caravan	=	5
All three magazines	=	3

Find; How many read none of the magazines? How many read caravan as their only magazines? How many read science today if and only if they read caravan?

Solution: Lets define:

$S =$ Set of those families that read Science today

$R =$ Set of those families that read readers digest

$C =$ Set of those families that read caravan

We want to find $n(S' \cap R' \cap C')$. Let:

$$U = \text{Set of all the families being questioned}$$

Now:

$$S' \cap R' \cap C' = (S \cup R \cup C)' = U - (S \cup R \cup C) \tag{2.9.43}$$

Therefore:

$$n(S' \cap R' \cap C') = n(U) - n(S \cup R \cup C) = 100 - n(S \cup R \cup C) \tag{2.9.44}$$

Now:

$$n(S \cup R \cup C) = 30 + 28 + 42 - 8 - 10 - 5 + 3 = 80 \tag{2.9.45}$$

So;

$$n(S' \cap R' \cap C') = 100 - 80 = 20 \tag{2.9.46}$$

So we have found that 20 families out of 100 have read all three magazines. Next we want to find $n(C - (R \cup S))$:

$$\begin{aligned} n(C - (R \cup S)) &= n(C) - n(C - \cap(R \cup S)) \\ &= n(C) - n((C \cap R) \cup (C \cap S)) \\ &= n(C) - n(C \cap R) - n(C \cap S) + n(C \cap K \cap S) \\ &= 42 - 10 - 5 + 3 = 30 \end{aligned} \tag{2.9.47}$$

So 30 people read only caravan. Finally we want to find $n((S \cap C) - R)$:

$$n((S \cap C) - R) = n(S \cap C) - n(S \cap C \cap R) = 5 - 3 = 2 \tag{2.9.48}$$

2 people read science today if and only if they read caravan.

Example 45

Problem: In a survey conducted of women it was found that:
There are more single then married women in south Delhi.
There are more married women who own cars then unmarried women without them.
There are fewer single women who own cars and houses then married women without cars and houses.
Is the number of single women who own cars and do not own homes greater than the number of married women who do not own cars but do own homes?

Solution: Lets define:

$$\begin{aligned} D &= \text{Set of married women} \\ K &= \text{Set of women who own cars} \\ C &= \text{Set of women who own homes} \end{aligned}$$

Then, the given conditions are:

$$n(D') > n(D) \tag{2.9.49}$$

$$n(D \cap k) > (D' \cap K') \tag{2.9.50}$$

$$n(D \cap K' \cap C') > n(D' \cap K \cap C) \tag{2.9.51}$$

We want to find $n(D' \cap K \cap C')$ and $n(D \cap K' \cap C)$. Let:

$$U = \text{Set of all women being questioned}$$

Now:

$$D' = D' \cap U = D' \cap (K \cup K') = (D' \cap K) \cup (D' \cap K') \tag{2.9.52}$$

$$D = D \cap U = D \cap (K \cup K') = (D' \cap K) \cup (D \cap K') \tag{2.9.53}$$

So:

$$n(D') = n(D' \cap K) + n(D' \cap K') \tag{2.9.54}$$

$$n(D) = n(D \cap K) + n(D \cap K') \tag{2.9.55}$$

But we know from Eq 2.9.49 that:

$$n(D' \cap K') + n(D' \cap K') > n(D \cap K) + n(D \cap K') \tag{2.9.56}$$

and by Eq 2.9.50:

$$n(D' \cap K) + n(D' \cap K') > n(D \cap K) + n(D \cap K') > n(D' \cap K') + n(D \cap K') \tag{2.9.57}$$

Therefore:

$$n(D' \cap K) > n(D \cap K') \tag{2.9.58}$$

Also:

$$\begin{aligned} D' \cap K &= (D' \cap K) \cap (C \cup C') \\ &= (D' \cap K \cap C) \cup (D' \cap K \cap C') \end{aligned} \tag{2.9.59}$$

and

$$\begin{aligned} D \cap K' &= (D \cap K') \cap (C \cup C') \\ &= (D \cap K' \cap C) \cup (D \cap K' \cap C') \end{aligned} \tag{2.9.60}$$

So:

$$n(D \cap K) = n(D' \cap K \cap C) + n(D' \cap K \cap C') \tag{2.9.61}$$

$$n(D \cap K') = n(D \cap K' \cap C) + n(D \cap K \cap C') \tag{2.9.62}$$

Now using the final condition we get:

$$n(D \cap K \cap C) + n(D' \cap K \cap C') > n(D \cap K' \cap C) + n(D' \cap K \cap C) \tag{2.9.63}$$

Which can also be written as:

$$n(D' \cap K \cap C') > n(D \cap K' \cap C) \tag{2.9.64}$$

So the number of single women who own cars and do not own a home is greater than the number of married women who do not own cars but own homes.

2.10 Cartesian product of two sets

Let D and K be two sets. The set of all ordered pairs (d, k) such that:

$$d \in D \tag{2.10.1}$$

$$k \in K \tag{2.10.2}$$

is called the *Cartesian* product of D and K and is denoted by:

$$D \times K \tag{2.10.3}$$

I must stress here that the ordered pair (d, k) is not the same as the set $\{d, k\}$. Two ordered pairs (d, k) and (x, y) are equal if and only of:

$$d = x \tag{2.10.4}$$

$$k = y \tag{2.10.5}$$

In any ordered pair of the form (d, k), d is called the first coordinate and k is the second coordinate.

Example 46

Problem: Lets define:

$$D = \{1, 2, 3\} \tag{2.10.6}$$

$$K = \{4, 5\} \tag{2.10.7}$$

Find; $D \times K$ and $K \times D$.

Solution:

$$D \times K = \{(1, 4), (1, 5), (2, 4), (2, 5), (3, 4), (3, 5)\} \tag{2.10.8}$$

$$K \times D = \{(4, 1), (5, 1), (4, 2), (5, 2), (4, 3), (5, 3)\} \tag{2.10.9}$$

This shows that:

$$D \times K \neq K \times D \tag{2.10.10}$$

In other words the operation of the Cartesian product does not commute.

Example 47

Problem: Let D be any set. Probe that:

$$D \times \emptyset \quad \text{and} \quad \emptyset \times D \tag{2.10.11}$$

are empty set.

Solution: Suppose $D \times \emptyset$ is not an empty set, then there is some x such that:

$$x \in D \times \emptyset \tag{2.10.12}$$

By definition $x = (d, k)$ where $d \in D$, $k \in \emptyset$. There is no point in this exercise as there is nothing in k. So we get:

$$D \times \emptyset = \emptyset \quad \text{and} \quad \emptyset \times D = \emptyset \tag{2.10.13}$$

Example 48

Problem: Let D, K, C be three sets. Then:

$$D \times (K \cup C) = (D \times K) \cup (D \times C) \tag{2.10.14}$$

Solution: Let:

$$x \in D \times (K \cup C) \tag{2.10.15}$$

Then, $x = (d, y)$ where $d \in D$, $y \in K \cup C$. Now if $y \in K$, then $x \in D \times K$. If $y \in C$, then $x \in D \times C$. In any case, $x \in (D \times K) \cup (D \times C)$. Therefore;

$$D \times (K \cup C) \subseteq (D \times K) \cup (D \times C) \tag{2.10.16}$$

Similarly:

$$(D \times K) \cup (D \times C) \subseteq D \times (K \cup C) \tag{2.10.17}$$

This proves the result.

Example 49

Problem: Let D, K, C be three sets. Prove:

$$D \times (K - C) = (D \times K) - (D \times C) \tag{2.10.18}$$

Solution: Let:

$$(d, y) \in D \times (K - C) \tag{2.10.19}$$

Then:

$$d \in D, y \in K, y \notin C \tag{2.10.20}$$

So:

$$(d, y) \in D \times K \quad \text{and} \quad (d, y) \notin D \times C \tag{2.10.21}$$

Therefore:

$$(d, y) \in (D \times K) - (D \times C) \tag{2.10.22}$$

This proves that:

$$D \times (K - C) \subseteq (D \times K) - (D \times C) \tag{2.10.23}$$

To prove the other side containment we proceed as we did above. Let:

$$x \in (D \times K) - (D \times C) \tag{2.10.24}$$

Then x is an element of $D \times K$ but it does not belong to $D \times C$. This means that:

$$x = (d, k) \tag{2.10.25}$$

where, $d \in D$ $k \in K$ but $k \notin C$. Otherwise:

$$x = (d, k) \in D \times C \tag{2.10.26}$$

This implies that:

$$k = K - C \tag{2.10.27}$$

Therefore:

$$x \in D \times (K - C) \tag{2.10.28}$$

Hence:

$$(D \times K) - (D \times C) \subseteq D \times (K - C) \tag{2.10.29}$$

Example 50

Problem: If the set D has m elements and the set K has n elements, how many elements does $D \times K$ have?

Solution: Let $d \in D$. Then the number of elements of $D \times K$ with first coordinate d, is n. But d can be chosen in m ways. So, the number of distinct elements in $D \times K$ is $m \times n$.

Example 51

Problem 1: If;

$$D = \{1, 4\} \tag{2.10.30}$$

$$K = \{4, 5\} \tag{2.10.31}$$

$$C = \{5, 7\} \tag{2.10.32}$$

Find, $D \times K) \cup (D \times C)$.

Solution 1: We know that:

$$(D \times K) \cup (D \times C) = D \times (K \cup C) \tag{2.10.33}$$

Now,

$$K \cup C = \{4, 5, 7\} \tag{2.10.34}$$

So,

$$D \times (K \cup C) = \{(1, 4), (4, 4), (1, 5), (4, 5), (1, 7), (4, 7)\} = (D \times K) \cup (D \times C) \tag{2.10.35}$$

Problem 2: Find $(D \times K) \cap (D \times C)$

Solution 2: Now:

$$D \times K = \{(1, 4), (4, 4), (1, 5), (4, 5)\} \tag{2.10.36}$$

$$D \times C = \{(1, 5), (1, 7), (4, 5), (4, 7)\} \tag{2.10.37}$$

So:

$$(D \times K) \cap (D \times C) = \{(1, 5), (4, 5)\} \tag{2.10.38}$$

2.11 Relation

Let D and K be two sets. A relation, R, from D to K is a subset of the cartesian product $D \times K$. If $(d, k) \in R$ then it is also denoted by:

$$dRk \tag{2.11.1}$$

and similarly dRk means $(d, k) \in R$. The symbol dRk is read as; 'd is related to b'. If $D = K$, we shall say R is a relation in D instead of 'from D to D'. Let $D = \{1, 2\}, K = \{3\}$.
Then:

$$R_1 = \{(1, 3), (2, 3)\} \tag{2.11.2}$$

$$R_2 = \{(1, 3)\} \tag{2.11.3}$$

$$R_3 = \{(2, 3)\} \tag{2.11.4}$$

are different relations from D to K. Suppose D is a non-empty set. A relation between R and D is called:
Reflexive: if $(d, d) \in R$ for all $d \in D$
Symmetric: if whenever $(d, k) \in R$ then $(k, 0) \in R$
Anti-symmetric: if $(d, k) \in R, (d, k) \in R \Rightarrow d = k$
Transitive: if whenever $(d, k), (k, c) \in R$ then $(d, c) \in R$.

A relation R is called an equivalence relation if it is reflexive, symmetric and transitive. A relation R on a set D is called a partial order relation, if it is reflexive, anti-symmetric and transitive.

Example 52

Problem 1: Lets define:

$$D = \{1, 2, 3\} \tag{2.11.5}$$

What type of relation is:

$$R_1 = \{(1, 1), (2, 2), (3, 3), (1, 3)\} \tag{2.11.6}$$

Solution 1: This relation is reflexive.

Problem 2:

$$R_2 = \{(1, 1), (2, 2)\} \tag{2.11.7}$$

Solution 2: Is not reflexive.

Problem 3:

$$R_3 = \{(1, 2), (2, 1)\} \tag{2.11.8}$$

Solution 3: Is symmetric but not reflexive.

Problem 4:

$$R_4 = \{(1, 1), (1, 2)\} \tag{2.11.9}$$

Solution 4: Is neither reflexive nor symmetric but is transitive.

Example 53

Problem: If:

$$Z = \text{Set of integers} \tag{2.11.10}$$

then the usual $\geq$ is partial order relation on Z as it is:

Reflexive, as $d \geq d$ for all $d \in Z$.

Anti-symmetric, as $d \geq k$, $k \geq d \Rightarrow d = k$.

Transitive, as $d \geq k, k \geq c \Rightarrow d \geq C$.

Example 54

Problem: Let D be the set of all lines in a plane. Let $R \subseteq DD$ where $R = \{(l,m)|l, m \in D, l||m\}$ then what type of relation is R?

Solution: Reflexive, as $(l,l) \in R$ for all $l \in D$ as $l||l$ for all $l \in D$.
Symmetric as if $(l,d) \in R$, then:

$$l||d \rightarrow m||l \rightarrow (m,l) \in R \tag{2.11.11}$$

Transitive, as if $(l,m) \in R, (m,n) \in R$ then $l||m, m||n \rightarrow (l,n) \in R$. Thus, the relation of parallelism is an *equivalence* relation.

2.11.1 Representation of a relation by a matrix

Sometimes, a relation is represented by a matrix where first we draw a table, suppose, R is a relation from a finite set D to a finite set K. We first construct a table by writing a all the elements D as a column on left and all the elements of K as the top row. Now if $(d_i, k_j) \in R$, i.e.. $(d_i R k_j)$ then we write 1 in the i^{th} row and j^{th} column. If $(d_i, k_j) \in R$ we write 0.
Suppose:

$$D = \{d_1, d_2, d_3, d_4\} \tag{2.11.12}$$

$$K = \{k_1, k_2, k_3\} \tag{2.11.13}$$

Then:

$$\begin{aligned} D \times K \quad = \quad & \{(d_1,k_1),(d_1,k_2),(d_1,k_3),(d_2,k_1),(d_2,k_2),(d_2,k_3),(d_3,k_1),(d_3,k_2) \\ & ,(d_3,k_3),(d_4,k_1),(d_4,k_2),(d_4,k_3)\} \end{aligned} \tag{2.11.14}$$

Suppose:

$$R = \{d_1,k_1),(d_1,k_2),(d_2,k_2),(d_3,k_3),(d_4,k_1)\} \tag{2.11.15}$$

Then in the matrix representation:

$$R = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

The above representation of a relation by the relation matrix has an advantage as just a quick look at it gives us some information about the relation. For instance, if the diagonal entries in the matrix are all 1 then the corresponding relation is reflexive. Again if the relation matrix is symmetric the corresponding relation is also symmetric. Similarly, if the relation happens to be anti-symmetric then in the relation-matrix if $a_{ij} = 1$ then $a_{ji} = 0 (i \neq j)$.

2.11.2 Diagrammatical representation of a relation

Sometimes a relation is represented with the help of a diagram called the graph of the relation. All we do in this representation is that we represent the elements of the set in the relation by dots called *nodes*. If dRk we join d and k by an arc and put an arrow from d to k. In case kRd also holds we draw another arc from k to d and put an arrow showing d being joined to d (which will look like a loop). Thus, if a relation is reflexive, there will be loops at all nodes:

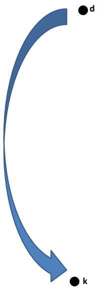

Figure 20: dRk

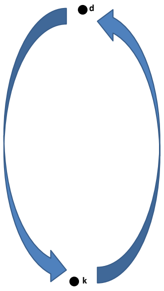

Figure 21: dRk, kRd

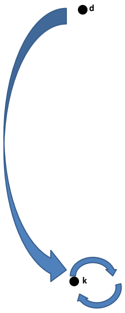

Figure 22: dRk, kRk

2.12 Mapping

Let D and K be two sets. A napping (or function) f from D to K is a relation from D to K such that to each $d \in D$ there exists a unique $k \in K$. In other words f is a subset of $D \times K$ such that $(d, k_1) \in f$ and $(d, k_2) \in f$ and for each of $d \in D$, there is some $k \in K$ such that $k_1 = k_2$, $(d, k) \in f$. A mapping f from D to K is denoted by:

$$f : D \to K \tag{2.12.1}$$

D is called the *domain* of f.
K is called the *Co-domain* of f.

Image of f is the set of these elements $k \in K$ such that:

$$(d, k) \in f \tag{2.12.2}$$

for some:

$$d \in D \tag{2.12.3}$$

It is denoted by $Im(f)$. If:

$$f : D \to K \tag{2.12.4}$$

and

$$(d, k) \in f \tag{2.12.5}$$

then we write:

$$k = f(d) \tag{2.12.6}$$

and k is called the image of d under f. Also, d is called pre-image of k under f. Note that the image of every element in D is unique.

Example 55

Problem: Lets define:

$$D = \{1, 2, 3\}$$

$$K = \{4, 5\}$$

Define:

$$f = \{(1, 4), (2, 5), (3, 4)\}$$

Then f is a mapping from D to K. But:

$$g = \{(1, 4), (2, 5), (3, 5), (1, 5)\} \tag{2.12.7}$$

Is not a mapping from D to K as two elements 4 and 5 in K are assigned to the element $1 \in D$. Again:

$$h = \{(1, 4), (2, 5)\} \tag{2.12.8}$$

is not a mapping as:

$$Dom(h) = \{1, 2\} \neq D \tag{2.12.9}$$

2.12.1 One-One mapping

A mapping: f: D $\rightarrow K$
is said to be one-one (1 to 1) if:

$$f(d_1) = f(d_2) \tag{2.12.10}$$

implies $d_1 = d_2$ where $d_1 \in D, d_2 \in D$. This is also sometimes called injective mapping. In other words, a mapping:

$$f : D \rightarrow K \tag{2.12.11}$$

is one-one if and only if:

$$d_1 \neq d_2(d_1 \in D, d_2 \in D) \tag{2.12.12}$$

then:

$$f(d_1) = f(d_2) \tag{2.12.13}$$

i.e images of distinct elements in D are distinct.

2.12.2 Onto mapping

A mapping:

$$f : D \rightarrow K$$

is said to be *onto* if given $k \in K$ there exists $d \in D$ such that $f(d) = k$. It is also sometimes called *surjective* mapping.

Example 56

Lets define:

$$D = \{1, 2, 3\} \tag{2.12.14}$$

$$K = \{4, 5\} \tag{2.12.15}$$

$$f = \{(1, 4), (2, 4), (3, 5)\} \tag{2.12.16}$$

Then $f : 0 \rightarrow K$ such that f is not one-one as $f(1) = 4$ and $f(2) = 4$. But $1 \neq 2$, f is onto as both 4 and 5 have pre-images in D namely 1 and 3.

Example 57

Lets define:

$$D = \{1, 2, 3\} \tag{2.12.17}$$

$$K = \{4, 5, 6, 7\} \tag{2.12.18}$$

$$f = \{(1,4),(2,5),(3,6)\} \tag{2.12.19}$$

Then:

$$f : D \to K \tag{2.12.20}$$

such that f is one-one as distinct elements in D have distinct images K, f is not onto as 7 has no pre-image in D.

Example 58

Lets define:

$$D = \{1,2,3\} \tag{2.12.21}$$

$$K = \{4,5,6\} \tag{2.12.22}$$

$$f = \{(1,6),(2,4),(3,5)\} \tag{2.12.23}$$

Then, $f : D \to K$ such that f is neither one-one nor onto.

Example 59

Lets define:

$$D = \{1,2,3\} \tag{2.12.24}$$

$$K = \{4,5,6\} \tag{2.12.25}$$

$$f = \{(1,4),(2,4),(3,5)\} \tag{2.12.26}$$

Then $f : D \to K$ such that f is neither one-one nor onto.

Example 60

Problem: Prove that if:

$$f : DK \tag{2.12.27}$$

such that f is onto, then $Im(f) = K$.

Solution: By definition:

$$Im(f) \subseteq K \tag{2.12.28}$$

Let $k \in K$. Therefore there exists $d \in D$ such that:

$$f(d) = k \quad \text{as } f \text{ is onto} \tag{2.12.29}$$

This implies:

$$k \in Im(f) \tag{2.12.30}$$

So;

$$K \subseteq Im(f) \tag{2.12.31}$$

Hence $Im(f) = K$.

2.12.3 Binary composition

A binary composition (or binary operator) on a set S is a rule which assigns to each pair of elements d, k of S a unique element c of S.

2.13 Boolean Algebra

A Boolean algebra is a set K of elements $x, y, z...$ together with two binary operations $+$ and $\cdot$ in K such that the following axioms hold:

- *Distributive laws*: For any $x, y \in K$:

  $$x \cdot (y + z) = x \cdot y + x \cdot z \tag{2.13.1}$$

  and

  $$x + (y \cdot z) = (x + y) \cdot (x + z) \tag{2.13.2}$$

- *Commutative laws*: For any $x, y, z \in K$:

  $$x + y = y + x \tag{2.13.3}$$

  and

  $$x \cdot y = y \cdot x \tag{2.13.4}$$

- *Identity*: There exists $0 \in K$ and $1 \in K$ which are called the zeroth element and unit element respectively, such that for all $x \in K$:

  $$x + 0 = x \tag{2.13.5}$$

  $$x \cdot 1 = x \tag{2.13.6}$$

- *Complement*: For each $x \in K$, there exists $x' \in K$, called the *complement* of x such that:

  $$x + x' = 1 \tag{2.13.7}$$

  and

  $$x \cdot x' = 0 \tag{2.13.8}$$

Now lets prove the results which can be easily deduced from the definition of Boolean algebra.

Example 61

Problem: Prove that both identity elements, 0 and 1 of K are unique.

Solution: Suppose there exists two zero elements 0_1 and 0_2. Then:

$$0_1 + 0_2 = 0_1 \tag{2.13.9}$$

and

$$0_2 + 0_1 = 0_2 \tag{2.13.10}$$

So by the commutative law:

$$0_1 = 0_2 \tag{2.13.11}$$

Hence the zero element of K is unique. The uniqueness of the unit element can be proven in a similar way.

Example 62

Problem: Prove that any complement x' for x in K is unique.

Solution: Suppose x'_1 and x'_2 are two complements of x in K. Then:

$$x + x'_1 = 1 \tag{2.13.12}$$

$$x + x'_2 = 0 \tag{2.13.13}$$

and therefore:

$$\begin{aligned} x'_1 &= x'_1 \cdot 1 \\ &= x'_1 \cdot (x + x'_2) \\ &= (x'_1 \cdot x) + (x'_1 \cdot x'_2) \\ &= (x \cdot x'_1) + (x'_1 \cdot x'_2) \\ &= 0 + (x'_1 \cdot x'_2) \\ &= (x'_1 \cdot x'_2) + 0 \\ &= (x'_1 \cdot x'_2) \end{aligned} \tag{2.13.14}$$

Similarly:

$$\begin{aligned} x_2' &= x_2' \cdot 1 \\ &= x_2' \cdot (x + x_1') \\ &= (x_2' \cdot x) + (x_2' \cdot x_1') \\ &= (x \cdot x_2') + (x_1' \cdot x_2') \\ &= 0 + (x_1' \cdot x_2') \\ &= (x_1' \cdot x_2') + 0 \\ &= (x_1' \cdot x_2') \end{aligned} \tag{2.13.15}$$

This shows $x_1' = x_2'$ i.e complement of any element in K is unique.

Example 63

Problem:Prove that each of the identity element in K is the complement of the other.

Solution: We want to show that $0' = 1$ and $1' = 0$. Now:

$$0' + 0 = 0' \tag{2.13.16}$$

and

$$0 + 0' = 1 \tag{2.13.17}$$

using the commutative law we get:

$$0' = 1 \tag{2.13.18}$$

Also,

$$1' \cdot 1 = 1' \tag{2.13.19}$$

and

$$1 \cdot 1 = 0 \tag{2.13.20}$$

this gives $1' = 0$.

Example 64

Problem: Prove that for any x in K:

$$(x')' = x \tag{2.13.21}$$

Solution: Now:

$$x + x' = 1 \tag{2.13.22}$$

and

$$x \cdot x' = 0 \tag{2.13.23}$$

implies that $x' + x = 1$.

Example 65

Problem: Prove that indempotent laws:

$$x + x = x \tag{2.13.24}$$

and

$$x \cdot x = x \tag{2.13.25}$$

for all x in K.

Solution: Now

$$\begin{aligned} x &= x + 0 \\ &= x + (x \cdot x') \\ &= (x + x) \cdot (x + x') \\ &= (x + x) \cdot 1 = x + x \end{aligned} \tag{2.13.26}$$

The proof for $x \cdot x$ is similar.

Example 66

Problem 1: Show that $x + x = 1$ for any $x \in K$

Solution 1:

$$\begin{aligned} x + 1 &= (x + 1) \\ &= 1 \cdot (x + 1) \\ &= (x + x') \cdot (x + 1) \\ &= x + (x' + 1) \\ &= x + x' = 1 \end{aligned} \tag{2.13.27}$$

Problem 2: Show that:

$$x \cdot 0 = 0 \tag{2.13.28}$$

for all $x \in K$.

Solution:

$$\begin{aligned} x \cdot 0 &= (x \cdot 0) + 0 \\ &= 0 + (x \cdot 0) \\ &= (x \cdot x') + (x \cdot o) \\ &= x \cdot (x' + 0) \\ &= x \cdot x' = 0 \end{aligned} \tag{2.13.29}$$

Example 67

Problem 1: Prove the absorption law:

$$x + (x \cdot y) = x \tag{2.13.30}$$

Solution 1:

$$\begin{aligned} x + (x \cdot y) &= (x \cdot y) + x \\ &= (x + y) + (x \cdot 1) \\ &= x \cdot (y + 1) \\ &= x \cdot 1 = x \end{aligned} \tag{2.13.31}$$

Problem 2: Prove:

$$x \cdot (x + y) = x \tag{2.13.32}$$

Solution 2:

$$\begin{aligned} x \cdot (x + y) &= (x + y) \cdot x \\ &= (x + y) \cdot (x + 0) \\ &= x + (y \cdot 0) \\ &= x + 0 = x \end{aligned} \tag{2.13.33}$$

Example 68

Problem: Prove that if:

$$x + z = y + z \tag{2.13.34}$$

and

$$x \cdot z = y \cdot z \tag{2.13.35}$$

then $x = y$ where $x, y, z.. \in K$.

Solution:

$$\begin{aligned} x &= x \cdot (x + z) \\ &= x \cdot (y + z) \\ &= x \cdot y + x \cdot z \\ &= x \cdot y + y \cdot z \\ &= y \cdot x + y \cdot z \\ &= y \cdot (x + z) \\ &= y \cdot (y + z) \\ &= y \end{aligned} \tag{2.13.36}$$

Example 69

Problem: Prove that if:

$$y \cdot x = z \cdot x \tag{2.13.37}$$

and

$$y \cdot x' = z \cdot x' \tag{2.13.38}$$

then:

$$y = z \tag{2.13.39}$$

where $x, y, z \in K$.

Solution:

$$\begin{aligned} y &= y \cdot 1 \\ &= y \cdot (x + x') \\ &= y \cdot x + y \cdot x' \\ &= z \cdot x + z \cdot x' \\ &= z \cdot (x + x') \\ &= z \cdot 1 \\ &= z \end{aligned} \tag{2.13.40}$$

Example 70

Problem: Prove;

$$x + (y + z) = (x + y) + z \tag{2.13.41}$$

for all $x, y, z \in K$.

Solution: Lets define:

$$X = x + (y + z) \tag{2.13.42}$$

$$Y = (x + y) + z \tag{2.13.43}$$

Then:

$$\begin{aligned} X \cdot x &= (x + (y + z)) \cdot x \\ &= x \cdot (x + (y + z)) \\ &= x \end{aligned} \tag{2.13.44}$$

$$\begin{aligned} Y \cdot x &= ((x+y)+z)\cdot x \\ &= (x+y)\cdot x + z\cdot x \\ &= x\cdot(x+y)+z\cdot x \\ &= x + z\cdot x \\ &= x + x\cdot z \\ &= x\cdot 1 + x\cdot z \\ &= x\cdot(1+z) \\ &= x\cdot 1 \\ &= x \end{aligned} \tag{2.13.45}$$

So:

$$Y \cdot x = X \cdot x \tag{2.13.46}$$

Also:

$$\begin{aligned} X \cdot x' &= (x+(y+z))\cdot x' \\ &= (x+y)\cdot x' + z\cdot x' \\ &= (x\cdot x' + y\cdot x') + z\cdot x' \\ &= (0 + y\cdot x') + z\cdot x' \\ &= y\cdot x' + z\cdot z' = (y+z)\cdot x' \end{aligned} \tag{2.13.47}$$

So:

$$X \cdot x' = Y \cdot x' \tag{2.13.48}$$

Example 71

Problem: Prove that;

$$(x+y)' = x' \cdot y' \tag{2.13.49}$$

Solution: We want to show that x', y' is the complement of $(x+y)$. Consider:

$$\begin{aligned} (x+y)+(x'\cdot y') &= ((x+y)+x')\cdot((x+y)+y') \\ &= (x'+(x+y))\cdot(x+(y+y')) \\ &= ((x'+x)+y)\cdot(x+1) \\ &= ((x+x')+y)\cdot 1 \\ &= (x+x')+y \\ &= 1+y = y+1 = 1 \end{aligned} \tag{2.13.50}$$

Also

$$
\begin{aligned}
(x+y)\cdot(x'+y') &= (x'\cdot y')\cdot(x+y)\\
&= ((x'\cdot y')\cdot x)+((x'\cdot y')\cdot y)\\
&= (x\cdot(x'\cdot y'))+(x'\cdot(y'\cdot y))\\
&= ((x\cdot x')\cdot y')+(x'\cdot(y\cdot y'))\\
&= (0\cdot y')+(x'\cdot 0)\\
&= 0+0=0 \qquad (2.13.51)
\end{aligned}
$$

This shows $x'\cdot y'$ is a complement of $(x+y)$. But every element in K has a unique element.

2.13.1 Example of Boolean algebras

It can be easily show that the Algebra of statements under the binary relations $\wedge$ and $\vee$ is a Boolean algebra. Also, yhe algebra of sets under the operations $\cap$ and $\cup$ is a Boolean algebra. We give below a table of the examples of *Boolean* algebra in logic and set theory:

	Logic	Sets	Boolean algebra
Statements	d,k,r	D,K,C	x,y,z..
Operator 'OR'	d $\vee k$	D $\cup K$	x+y
Operator 'AND'	d $\wedge k$	D $\cap K$	x $\cdot y$
Operator 'NOT'	$\sim d$	D'	x'
Tautology	T	Universal set	1
Fallacy	F	$\emptyset$	0
Implication	d $\Rightarrow k$	Mapping	x' + y
Equivalence	d $\Leftrightarrow k, d\equiv k$	1-1 mapping	x $\cdot y + x'\cdot y'$

Table 32: Examples of Boolean algebras

Example 72

Problem: Using Boolean algebra, prove that:

$$d\wedge(d\Rightarrow k)\Rightarrow k \qquad (2.13.52)$$

is a tautology.

Solution: Using symbols '+' and '$\cdot'of Boolean algebra, the given statement can be written as :$

$$
\begin{aligned}
(x\cdot(x'+y))'+y &= (x\cdot x'+x\cdot y)'+y\\
&= (0+x\cdot y)'+y\\
&= (x\cdot y)'+y\\
&= (x'+y')+y\\
&= x'+(y'+y)\\
&= x'+x \qquad (2.13.53)
\end{aligned}
$$

This is obviously a tautology as $x' \neq 0$.

Example 73

Problem: Using Boolean algebra, show that:

$$\sim k \wedge (d \Rightarrow k) \Rightarrow \sim d \tag{2.13.54}$$

is a tautology.

Solution: Now the given statement can be written as:

$$\begin{aligned}(y' \cdot (x' + y))' + x' &= (y' \cdot x' + y' \cdot y)' + x' \\ &= (y' \cdot x' + 0)' + x' \\ &= (y + x) + x' \\ &= y + (x + x') \\ &= y + 1 = 1 \qquad (2.13.55)\end{aligned}$$

Which is also a tautology as $y \neq 0$.

Example 74

Problem: Using Boolean algebra determine the validity of the following argument:
The triangle is isosceles if and only if two of its sides are equal. No two sides of the triangle are equal. Therefore the triangle is not isosceles.

Solution: Suppose:

$$d = \text{The triangle is isosceles}$$

$$k = \text{Two sides of the triangle are equal}$$

The argument can be written in terms of logic as:

$$(d \Leftrightarrow k) \wedge \sim k \Rightarrow \sim d \tag{2.13.56}$$

In symbols of Boolean algebra, this may be written as:

$$\begin{aligned}((x \cdot y + x' \cdot y') \cdot y')' + x' &= (y' - (x \cdot y + x' \cdot y')) + x' \\ &= (y' \cdot (x \cdot y) + y' \cdot (x' \cdot y'))' + x' \\ &= ((y' \cdot y) \cdot c + y' \cdot (x' \cdot y'))' + x' \\ &= (0 + y' \cdot (x' \cdot y'))' + x' \\ &= y + (x + y) + x' \\ &= y + (x + x') \\ &= y + 1 = 1 \qquad (2.13.57)\end{aligned}$$

Which is a tautology therefore the given argument is not valid.

3 Groups, Rings and Fields

Now that we have learned about set theory, we will define more things in a similar way to sets. In set theory we defined operations that acted on sets to join two elements of the set to generate another *unique* element of the set. Now we shall define such systems as *Groups, Rings and Fields.* We shall briefly discuss another object called an *Integral domain*, which is a step up from rings and does not quite have the properties of a field. Of course all these terms are just mathematical definitions and one can go on defining an indefinite number of such things.

3.1 Introduction to Groups

Group theory was first used as part of *Geometry*, to manipulate objects and operations between them. They can be used in any part of mathematics and are firmly at the heart of modern mathematics. Group theory is also very useful in theoretical physics, which is the main reason I am studying the topic. So lets define a group now; G is said to form a group w.r.t an operator if the following conditions are satisfied:

- *Association Law*

$$a * (b * c) = (a * b) * c \qquad \forall a, b, c \in G \tag{3.1.1}$$

- *Existence of Identity*

  $\exists\ e \in G$, such that:

$$a * e = e * a = a \qquad \forall a \in G \tag{3.1.2}$$

- *Existence of Inverse*

  For every $a \in G$:

$$\exists\ a' \in G$$

  Such that:

$$a * a' = a' * a = e \tag{3.1.3}$$

  where e is the identity element.

- *Closure*

$$a, b \in G$$

  $a * b$ is a *unique* member of G:

$$a * b \in G \qquad \forall a, b \in G \tag{3.1.4}$$

The four equations, Eq 3.1.1, 3.1.2, 3.1.3, 3.1.4 are the defining equations for a group. In addition to these properties, if a group, G, has commutative property:

$$a * b = b * a \qquad \forall a, b \in G \tag{3.1.5}$$

Then the group is called a commutative group, also know in the literature as an *Abelian* group. The inverse is also true, a group that is non-commutative is called a *non-abelian group.* The most commonly used symbols for operators/-compositions are:

$$*, \oplus, \otimes, + \qquad etc$$

Now whenever we talk about a group we have to define a binary operation with it, as a group is only complete with a binary operation (without it, we just a set). A group which has finite number of elements is called (very creatively) a *finite group.* A group with an infinite number of elements, like a group containing all real numbers, is called, yup you guessed it! an *infinite group.* The best way to grasp these concepts (as with anything in mathematics) is through examples.

Example 1

Problem: Does the set Z of integers forms an abelian group w.r.t the addition, $+$, operator.

Solution: To check this claim, we have to see weather Z satisfies the properties of a group.
Closure $\Rightarrow$ If $a, b \in Z$ then $a + b$ is an integer therefore $a + b \in Z$ and hence the closure property is satisfied.
Associativity $\Rightarrow$ $a, b, c \in Z$ then:

$$a + (b + c) = (a + b) + c \tag{3.1.6}$$

This is true for any integers.
Identity $\Rightarrow$ This is given by:

$$a + \text{Identity} = a \tag{3.1.7}$$

It is clear that for the set of integers and the addition operator, the identity is 0.
Inverse $\Rightarrow$ If $a \in Z$ is any number, then $\exists - a \forall a \in Z$, such that:

$$a + (-a) = (-a) + a = 0 \tag{3.1.8}$$

So $-a$ is the inverse of a. Hence each element of Z has an inverse for the addition operator.
Commutativity $\Rightarrow$ We already know that Z is a group as it satisfies all the properties that are required. But we are told that the group is commutative, therefore we check that:

$$a + b = b + a, \qquad \forall\, a, b \in Z \tag{3.1.9}$$

which is true for any integer. So $\langle Z, +\rangle$ forms an abelian group.

Example 2

Problem: Check weather the set of all natural numbers, Q, forms a group with the addition operator.

Solution: Once again we check weather Q satisfies the properties of a group.
Closure $\Rightarrow a, b \in Q$:

$$a + b = c \tag{3.1.10}$$

Now since a and b are rational, which means they can written as fractions, c must also be a fraction since its comes from 2 numbers that are fractions. So the closure property is satisfied.
Associativity $\Rightarrow$ Natural numbers are fractions and fractions are always associative.
Identity $\Rightarrow$ At first sight we may think that there cannot be an identity, for how can 0 be a rational number, i.e

$$\frac{0}{0} = \text{Undefined} \tag{3.1.11}$$

but we can simply write fractions like:

$$\frac{0}{a} = 0 \qquad \forall a \in Q \tag{3.1.12}$$

And we know:

$$\frac{a_1}{a_2} + 0 = \frac{a_1}{a_2} \tag{3.1.13}$$

Therefore 0 is the identity.
Inverse $\Rightarrow$ For any rational number, $a \in Q$, we can write a as a fraction:

$$a = \frac{a_1}{a_2} \tag{3.1.14}$$

From the definition of fractions:

$$\left(\frac{a_1}{a_2}\right) + \left(-\frac{a_1}{a_2}\right) = 0 \tag{3.1.15}$$

Therefore the inverse is $\left(-\frac{a_1}{a_2}\right)$ $\forall a_1, a_2, \in Q$.
Commutativity $\Rightarrow$ This simply follows from the addition of numbers:

$$\frac{a_1}{a_2} + \frac{b_1}{b_2} = \frac{b_1}{b_2} + \frac{a_1}{a_2} \tag{3.1.16}$$

So $\langle Q, +\rangle$ is an abelian group.

Example 3

Problem : Check $\langle Q', \cdot\rangle$, where Q' is the set of all non-zero rational numbers, forms a abelian group.

Solution: Following from Example 2. The closure and associativity are simple and follow from the definitions of fractions. The only difference from Example 2 is that the identity in this case is 1 and for and for any $a \in Q'$ the inverse is $\frac{1}{a}$. Therefore $\langle Q', \cdot \rangle$ is an abelian group.

Example 4

Problem: Check weather the following forms a group and weather it is commutative:

$$\langle \Re, + \rangle \qquad \Re \text{ is the set of all real numbers} \tag{3.1.17}$$

Solution: This can also be checked with the axiomatic properties and it is easy to show that $\langle \Re, + \rangle$ forms an Abelian group.

Example 5

Problem: Check weather the following is a group and weather it commutes:

$$\langle G, \cdot \rangle \tag{3.1.18}$$

where:

$$G = \{1, -1\} \tag{3.1.19}$$

Solution: Lets check weather G satisfies the axioms:
Closure ⇒

$$\begin{aligned} 1 \cdot 1 &= 1 \quad \in G \\ 1 \cdot (-1) &= -1 \quad \in G \\ (-1) \cdot (-1) &= 1 \quad \in G \end{aligned} \tag{3.1.20}$$

So the closure property holds.
Associativity ⇒

$$\begin{aligned} 1 \cdot (1 \cdot 1) &= (1 \cdot 1) \cdot 1 \\ -1 \cdot (1 \cdot 1) &= (-1 \cdot 1) \cdot 1 \\ -1 \cdot (-1 \cdot 1) &= (-1 \cdot -1) \cdot 1 \\ -1 \cdot (-1 \cdot -1) &= (-1 \cdot -1) - 1 \end{aligned} \tag{3.1.21}$$

and so on.. Therefore associativity holds.
Identity ⇒

$$\begin{aligned} 1 \cdot 1 &= 1 \quad (1 = \text{identity}) \\ -1 \cdot 1 &= 1 \quad (1 = \text{identity} \end{aligned} \tag{3.1.22}$$

Therefore identity is always present.
Inverse ⇒

$$\begin{aligned} 1 \cdot 1 &= 1 \quad (1 = \text{inverse}) \\ -1 \cdot -1 &= 1 \quad (-1 = \text{inverse}) \end{aligned} \tag{3.1.23}$$

Therefore the inverse is always present.
Commutativity ⇒

$$\begin{aligned} 1 \cdot 1 &= 1 \cdot 1 \\ -1 \cdot 1 &= 1 \cdot -1 \\ -1 \cdot -1 &= -1 \cdot -1 \end{aligned} \tag{3.1.24}$$

Therefore commutativity holds. Hence $\langle G, \cdot \rangle$ forms an Abelian group.

Example 6

Problem: If $G = \{a\}$ and an operation is defined as:

$$a * a = a \qquad \forall a \in G \tag{3.1.25}$$

Check weather $\langle G, * \rangle$ forms a group and weather it is abelian or not.

Solution: Well this is really easy, since the closure property is given in the definition of the operator. a is its own identity and inverse by the same definition and so:

$$a * a = a = a * a \tag{3.1.26}$$

Since there is only one element in the group!. So $\langle G, * \rangle$ forms an abelian group.

Example 7

Problem: Check

$$\langle Z, \cdot \rangle \tag{3.1.27}$$

where Z is the set of all integers and $\cdot$ is the usual multiplication operator.

Solution: It is easy to see that '$\cdot$' is a binary composition on Z. So closure holds, we also know the following properties of integers:

$$\begin{aligned} a \cdot (b \cdot c) &= (a \cdot b) \cdot c \qquad \forall a, b, c \in Z \\ a \cdot b &= b \cdot a \\ a \cdot 1 &= 1 \cdot a = a \end{aligned} \tag{3.1.28}$$

So associativity and commutation also holds along with the identity, I. Now lets see if there is an inverse, consider:

$$2 \cdot a = 1 \tag{3.1.29}$$

the only possible value for $a = \frac{1}{2}$, which is not an element of the group as it is not an integer, so there is no inverse. Hence $\langle Z, \cdot \rangle$ is not a group[1].

Example 8

Problem: Check

$$\langle Q, \cdot \rangle \qquad Q = \text{all rational numbers} \tag{3.1.30}$$

Solution: All axioms hold except that there is no inverse for 0, so it is not a group.

3.2 Properties

3.2.1 Identity element in a group, G, is unique

Suppose there are two identity elements; $e_1 \& e_2$, then we have:

$$\begin{aligned} a * e_1 &= a && (3.2.1) \\ a * e_2 &= a && (3.2.2) \end{aligned}$$

where $a \in G$. Therefore:

$$a * e_1 = a * e_2 \rightarrow e_1 = e_2 \tag{3.2.3}$$

However in the last step we have also made another assumption. The assumption that there exists a cancellation law. But this can also be proven.

3.2.2 Cancellation law

Consider $a, b, c \in G$:

$$\begin{aligned} a * c &= a * c \\ a^{-1} * (a * b) &= a^{-1} * (a * c) \\ (a^{-1} * a) * b &= (a^{-1} * a) * c \quad \Rightarrow \qquad \text{Associative law} \\ e * b &= e * c \qquad\quad e = \text{Identity} \\ b &= c && (3.2.4) \end{aligned}$$

Therefore we could just cancel the $a's$.

3.2.3 Inverse of each $a \in G$ is unique

Let $a \in G$ be some element and suppose it has two inverse elements, x and y:

$$\begin{aligned} ax &= xa = e && (3.2.5) \\ ay &= ya = e && (3.2.6) \end{aligned}$$

[1] Note that $\langle Z, + \rangle$ is a group

Now:

$$\begin{aligned} x &= xe \\ &= x(ay) \\ &= (xa)y \\ &= ey \\ &= y \end{aligned} \tag{3.2.7}$$

Therefore the inverse is always unique.

3.2.4 Inverse of an inverse, $(a^{-1})^{-1} = a$

Consider:

$$aa^{-1} = a^{-1}a = e \tag{3.2.8}$$

This means a is the inverse of a^{-1}, so it can be written as $a = (a^{-1})^{-1}$.

3.2.5 Associativity of inverse, $(ab)^{-1} = b^{-1}a^{-1}$

We want to show that when two elements are combined via an operation, the identity of this new element in just two identities of the two separate elements combined via the same operation:

$$\begin{aligned} (ab)(b^{-1}a^{-1}) &= (b^{-1}a^{-1})(ab) \\ &= e \end{aligned} \tag{3.2.9}$$

Suppose:

$$\begin{aligned} (ab)(b^{-1}a^{-1}) &= \left((ab)b^{-1}\right)a^{-1} \\ &= \left(a(bb^{-1})\right)a^{-1} \\ &= (ae)a^{-1} \\ &= eaa^{-1} \\ &= e \end{aligned} \tag{3.2.10}$$

And in exactly the same way one can get:

$$(b^{-1}a^{-1})(ab) = e \tag{3.2.11}$$

Example 9

Problem: Show that the set Q' of positive rational numbers forms an abelian group w.r.t the operation $*$ defined on it by:

$$a * b = \frac{ab}{2} \tag{3.2.12}$$

Solution: Lets take any two elements; $a, b \in Q'$.
Closure ⇒ Now

$$a * b = \frac{ab}{2} \tag{3.2.13}$$

Which will always be a positive rational number as the set only contains positive rational numbers and the product of two rational numbers is a positive rational number. As it is divided by two, it is a fraction therefore this is also a positive rational number for only a and b. Therefore the closure property holds.
Associativity ⇒ Consider $a, b, c \in Q'$:

$$\begin{aligned}(a * b) * c &= \left(\frac{ab}{2}\right) * c \\ &= \frac{abc}{4} \qquad (3.2.14)\end{aligned}$$

$$\begin{aligned}a * (b * c) &= a * \left(\frac{bc}{2}\right) \\ &= \frac{abc}{4} \qquad (3.2.15)\end{aligned}$$

Therefore:

$$(a * b) * c = a * (b * c) \tag{3.2.16}$$

Commutativity ⇒ This is easy to see, as the primary operation is a multiplication and we know that multiplication always commutes:

$$\begin{aligned}a * b &= \frac{ab}{2} \\ &= \frac{ba}{2} \\ &= b * a \qquad (3.2.17)\end{aligned}$$

Identity ⇒ Consider $a \in Q'$:

$$\begin{aligned}a * 2 &= \frac{a2}{2} \\ &= \frac{2a}{2} \\ &= a\end{aligned}$$

Therefore 2 is the identity $\forall a \in G$. Note that this would obviously be the case as the operations returns a result that has a number divided by 2, if it returned a number divided by 3, the identity would be 3 and so on.
Inverse ⇒ Consider $a \in Q'$; we want to show:

$$a * a^{-1} = a^{-1}a = 2 \tag{3.2.19}$$

Therefore:

$$a * a^{-1} = \frac{a^{-1}a}{2} \tag{3.2.20}$$

Rearranging, we get the inverse as:

$$a^{-1} = \frac{4}{a} \tag{3.2.21}$$

$\forall a \in G$. Therefore $\langle Q', *\rangle$ forms an Abelian group.

Example 10

Problem: If Z is the set of integers and $*$ is an operation defined by:

$$a * b = a + b + 1 \tag{3.2.22}$$

Where '+' is the usual addition, show that $\langle Z, *\rangle$ forms an abelian group.

Solution: *Closure* $\Rightarrow$ Let $a, b \in Z$ be any two elements:

$$a * b = a + b + 1 \tag{3.2.23}$$

Since $a + b$ are just numbers, adding 1 to the sum of integers will also give an integer, therefore:

$$a + b + 1 \in Z \tag{3.2.24}$$

$a, b \forall Z$.
Associativity $\Rightarrow$ Consider $a, b, c \in Z$:

$$\begin{aligned}(a * b) * c &= (a + b + 1) * c\\ &= (a + b + 1 + c + 1)\\ &= a + b + c + 2\end{aligned} \tag{3.2.25}$$

$$\begin{aligned}a * (b * c) &= a * (b + c + 1)\\ &= a + b + c + 1 + 1\\ &= a + b + c + 2\end{aligned} \tag{3.2.26}$$

Therefore:

$$(a * b) * c = a * (b * c) \tag{3.2.27}$$

Identity $\Rightarrow$ $e \in Z$ will be identity if:

$$a * e = a = e * a \tag{3.2.28}$$

Consider:

$$\begin{aligned}a * e &= a+e+1\\ a+e+1 &= a\\ e+1 &= 0\\ e &= -1 \qquad (3.2.29)\end{aligned}$$

Therefore -1 is the identity.
Inverse $\Rightarrow$ Consider $a \in Z$; the condition for the inverse is:

$$a * a^{-1} = a^{-1}a = -1 \qquad (3.2.30)$$

Which is equivalent to:

$$a + a' + 1 = a' + a + 1 = -1 \qquad (3.2.31)$$

Therefore:

$$a' = -1 - 1 - a = -2 - a \qquad (3.2.32)$$

$-2 - a \in Z$ therefore a' is an inverse $\forall a \in Z$.
Commutativity $\Rightarrow$

$$\begin{aligned}a * b &= a+b+1\\ &= b+a+1\\ &= b * a \qquad (3.2.33)\end{aligned}$$

Therefore $\langle Z, *\rangle$ is an abelian group.

Example 11

Problem: Let Q be the set of rational numbers. Define:

$$G = \{(a,b)|a,b \in Q, a \neq 0\} \qquad (3.2.34)$$

Lets define the operator of G by:

$$(a,b) * (c,d) = (ac, ad+b) \qquad (3.2.35)$$

Show that $\langle G, *\rangle$ forms a non-abelian group.

Solution:
Closure $\Rightarrow Supposewehavetwoelements:$

$$(a,b),(c,d) \in G \qquad (3.2.36)$$

Remember $a, c \neq 0$. Using the operation:

$$(a,b) * (c,d) = (ac, ad+b) \qquad (3.2.37)$$

But $(ac, ad+b) \in G \forall a,b,c,d$. Now as $a \& c \neq 0$, this means $ac \neq 0$. Therefore closure holds.

Associativity ⇒ This property is obvious as the operation defined between only two elements, $(a,b)\&(c,d)$.
Identity ⇒ We want to show:

$$(a,b)*(c,d)=(a,b) \tag{3.2.38}$$

Which is equivalent to:

$$(ac,ad+b)=(a,b) \tag{3.2.39}$$

Therefore d must be zero since a cannot be zero and form this requirement, c must be 1 to satisfy the above condition. Therefore $(1,0)$ is the identity $\forall(a,b)\in G$.
Inverse ⇒ The inverse requirement is:

$$(a,b)*(c,d)=(1,0) \qquad \forall a,b,c,d\in G \tag{3.2.40}$$

So lets use the operation:

$$(a,b)*(c,d)=(ac,ad+b)=(1,0) \tag{3.2.41}$$

Therefore $c=\frac{1}{a}$ and $-\frac{b}{a}=d$ and:

$$\left(\frac{1}{a},-\frac{b}{a}\right)=\text{Inverse} \tag{3.2.42}$$

$\forall a,b\in G$.
Commutativity ⇒ The condition is:

$$(a,b)*(c,d)=(c,d)*(a,b) \tag{3.2.43}$$

$$(ac,ad+b)=(ca,cb+d) \tag{3.2.44}$$

$\forall a,b,c,d\in G$. So to disprove this we just need to find one set of elements that dissatisfy this condition; so consider:

$$(2,3),(1,4)\in G \tag{3.2.45}$$

Now:

$$\begin{aligned}(2,3)*(1,4) &= (2\times 1, 8+3)\\ &= (2,11)\end{aligned} \tag{3.2.46}$$

$$\begin{aligned}(1,4)*(2,3) &= (1\times 2, 3+4)\\ &= (2,7)\end{aligned} \tag{3.2.47}$$

But $(2,11)\neq(2,7)$. Therefore commutativity is not satisfied and $\langle G,*\rangle$ is a non-abelian group.

Example 12

Problem: Give an example of a system $\langle G, * \rangle$ which satisfies all of the axioms in the definition of a group, except associativity axiom, i.e:

$$(a * b)^{*} c \neq a * (b * c) \qquad \forall\, a, b, c \in G \tag{3.2.48}$$

Solution: There is no specific method that can be used to solve this problem (I dont think!). The crucial thing here is how the operator is defined. Suppose its defined as:

$$a * b = a - b \tag{3.2.49}$$

Then we have:

$$\begin{aligned} (a * b) * c &= (a - b) * c \\ &= (a - b) - c \\ &= a - b - c \end{aligned} \tag{3.2.50}$$

$$\begin{aligned} a * (b * c) &= a * (b - c) \\ &= a - (b - c) \\ &= a - b + c \end{aligned} \tag{3.2.51}$$

Therefore:

$$a - b - c = a - b + c \tag{3.2.52}$$

But if $a, b, c \in G$ and I define G to be the group of all real integers then Eq 3.2.52 is obviously not true. Hence the associativity condition is not satisfied, it is easy to check that all the other properties are satisfied.

Example 13

Problem: Show that the set:

$$G = \{1, -1, i, -i\} \tag{3.2.53}$$

forms an abelian group w.r.t the usual multiplication operator.

Solution: When there are a small amount of elements in a group, one can draw a comparison table to check its properties:

	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

Table 33: Composition table for G

Closure⇒ It is easy to see as all the elements in the table are $\in G$.
Associativity⇒ Follows from the properties of the multiplication operator.
Commutativity⇒ Follows from the properties of the multiplication operator.
Identity⇒ Lets check the identity elements for each element individually:

$$*1 = 1 * 1 = 1 \tag{3.2.54}$$

therefore identity for 1 is 1 and $1 \in G$.

$$-1 * 1 = 1 * (-1) = (-1) \tag{3.2.55}$$

therefore identity for -1 is 1 and $1 \in G$. Similarly it is found that 1 is the identity for $i \& -i$.
Inverse⇒ Lets check the inverse for each elements:

$$i(-i) = 1 \tag{3.2.56}$$

The inverse of i is $-i$ and vice-versa.

$$(-1)(-1) = 1 \tag{3.2.57}$$

The inverse of (-1) is (-1).

$$(1)(1) = 1 \tag{3.2.58}$$

Therefore the inverse of 1 is 1. So we see that an inverse exist for each element, hence $\langle G, * \rangle$ is an abelian group.

Example 14

Problem: Let G be the set $\{e, a, b\}$ and let the operation on G be defined by the following composition table:

	e	a	b
e	e	a	b
a	a	e	a
b	b	b	e

Table 34: Composition table for G

Which may also be written as a set of equations:

$$\begin{aligned}e * e &= e\\ e * a &= a\\ e * b &= b\\ a * e &= a\\ a * a &= e\\ a * b &= a\\ b * e &= b\\ b * a &= b\\ b * b &= e\end{aligned}$$

Does $\langle G, * \rangle$ form a group?

Solution:
Closure⇒ This is obvious as all the elements in the table are $a, b, c \in G$.
Identity⇒ From the equations above we can see that e is the identity.
Inverse⇒ Looking at the equations e's inverse is e, a is the inverse of a and b is the inverse of b.
Associativity⇒ We want to check the condition:

$$a * (b * c) = (a * b) * a \tag{3.2.59}$$

Compute the L.H.S:

$$a * (b * c) = a * b = a \tag{3.2.60}$$

$$(a * b) * c = a * a = e \tag{3.2.61}$$

But $a \neq e$, therefore associativity does not hold and $\langle G, * \rangle$ is not a group.

Example 15

Problem: Define:

$$G = \{0, 1, 2, 3, 4\} \tag{3.2.62}$$

and the operator:

$$a * b = c \qquad\qquad \forall a, b \in G \tag{3.2.63}$$

where c is the least non-negative remainder for by dividing $a + b$ by 5. Show that $\langle G, * \rangle$ forms an abelian group.

Solution: Form the composition table:

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Table 35: Composition table for G

Closure⇒ We can see that all elements in the composition table are $\in G$, therefore closure holds.
Commutativity⇒ This is again trivial as the remainder got by dividing $a+b$ by 5 is the same as $b+a$ divided by 5 $\forall a, b \in G$.
Associativity⇒ Let:

$$a, b, c \in G \tag{3.2.64}$$

The condition for associativity is:

$$a * (b * c) = (a * b) * c \tag{3.2.65}$$

Define:

$$a * b = d \tag{3.2.66}$$

and

$$(a * b) * c = d * c = r \tag{3.2.67}$$

Now $a * b = d$, where d is the least non-negative remainder got by dividing $a+b$ by 5, which can be written as:

$$a + b = 5k_1 + d \tag{3.2.68}$$

where k_1 is an integer.
Again:

$$d * c = r \tag{3.2.69}$$

where r is the least non-negative remainder got by dividing $d+c$ by 5. This can be re-written as:

$$d + c = 5k_2 + r \tag{3.2.70}$$

So we get:

$$\begin{aligned}(a * b) * c &= d + 5k_1 + c \\ &= 5k_1 + r + 5k_2 \\ &= r + 5(k_1 + k_2) \\ &= 5k + r \end{aligned} \tag{3.2.71}$$

where $0 \leq r \leq 5$. So r is the least remainder got by dividing $(a+b)+c$ by 5. Similarly:

$$a * (b * c) \equiv 5 \tag{3.2.72}$$

then as shown above, s will be the remainder got by dividing $a+(b+c)$ by 5:. But sincel

$$(a+b)+c = a+(b+c) \tag{3.2.73}$$

the two remainders are the same:

$$r = s \tag{3.2.74}$$

Therefore:

$$(a * b) * c = a * (b * c) \tag{3.2.75}$$

and associativity holds.
Identity⇒ It is easy to see from the composition table that zero is the identity. This might be expected by an operation which primarily defined by addition.
Inverse⇒ The condition is:

$$a * b = 0 \qquad\qquad \forall a, b \in G \tag{3.2.76}$$

Note that:

$$0 * 0 = 0 \tag{3.2.77}$$

Therefore inverse of 0 is 0. Suppose $0 \neq a \in G$ be any element then $5 - a \in G$. So by definition:

$$(5-a) * a = a * (5-a) = 0 \tag{3.2.78}$$

Therefore $(5-a)$ is the inverse $\forall a \in G$ where $a \neq 0$. Therefore $\langle G, * \rangle$ is an abelian group. The above composition is called *addition modulo 5* and is sometimes defined by $\oplus_5$ such that:

$$3 \oplus_5 2 = 0 \tag{3.2.79}$$

This can be defined by this composition in general on a set $\{0, 1, 2, 3...(n-1)\}$ where it is called the *addition modulo n*.

Example 16

Problem: Let

$$G = \{1, 2, 3, 4, 5, 6\} \tag{3.2.80}$$

and define a binary composition on G:

$$a * b = c \tag{3.2.81}$$

where c is the least non-negative remainder obtained by dividing the product, ab, by 7. Show that $\langle G, * \rangle$ forms an abelian group.

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Table 36: Composition table for G

Solution: The composition table is:
Closure⇒ The closure property holds as all the elements in the composition table are in G.
Commutativity⇒ Easy to see from the table, also expected as primary operation in multiplication.
Associativity⇒ Easy to see from the composition table
Identity⇒ 1 is the identity
Inverse⇒ 1 is the inverse of 1, 2 of 2, 3 of 3 and so on..
Therefore $\langle G, * \rangle$ is an abelian group. This binary composition is called the *multiplication modulo 7* and is denoted by $\odot_7$ or X_7.

Example 17

Problem: Define:

$$S = \{x \in Z | 1 \leq x \leq n, \text{ where } (x,n) = 1\} \tag{3.2.82}$$

Z is the set of integers and (x,n) stands for the highest common factor (HCF) of x and n. Define a composition * on S as:

$$a * b = c \qquad\qquad \forall a, b \in S \tag{3.2.83}$$

where c is the least positive integer obtained as the remainder when ab is divided by n. Show that $\langle S, * \rangle$ forms an abelian group.

Solution:
Closure⇒ Let:

$$a * b = c \tag{3.2.84}$$

Then c cannot be zero otherwise n divides ab, which is not possible as $(a,n) = 1$ and $(b,n) = 1$. So $1 \leq c < n$. Further if $(c,n) \neq 1$ then there is some prime number p such that it divides both c and n, which means p divides ab as $a*b = c$ means that we can write it as:

$$ab = c + kp \tag{3.2.85}$$

for some integer k; p being a prime number, either p divides a or p divides v. Thus either p divides the HCF of a and n or HCF of b and n which is not possible as both $(a,b) = 1$ and $(b,n) = 1$; therefore:

$$(c, n) = 1 \tag{3.2.86}$$

and $c \in S$, therefore closure holds.
Associativity⇒ If:

$$\begin{aligned} a * b &= r_1 \\ (a * b) * c = r_2 \end{aligned}$$

Then

$$r_1 * c = r_2 \tag{3.2.87}$$

Which means:

$$r_1 c = r_2 + k_2 n \tag{3.2.88}$$

for some integer k_2 and similarly:

$$ab = r_1 + k_1 n \tag{3.2.89}$$

for some integer k_1 and:

$$r_1 c = r_2 + k_2 n \tag{3.2.90}$$

$$\Rightarrow (ab - k_1 n)c = r_2 + k_1 n \tag{3.2.91}$$

$$\Rightarrow (ab)c = r_2 + (k_2 + k_1 c)n \tag{3.2.92}$$

Which implies that r_2 is the least non-negative remainder get by dividing $(ab)c$ by n. Similarly if $a*(b*c) = r_3$ then r_3 is the least non-negative integer obtained as remainder when $a(bc)$ is divided by n. But:

$$\begin{aligned} (ab)c &= a(bc) \\ \Rightarrow r_2 &= r_3 \\ \Rightarrow (a * b) * c &= a * (b * c) \end{aligned} \tag{3.2.93}$$

Therefore associativity holds.
Identity⇒ $1 \in S$ and:

$$1 * a = a * 1 = a \qquad \forall a \in S \tag{3.2.94}$$

Therefore 1 is the identity.
Inverse⇒ Let $a \in S$, then $(a.n) = 1$. So there exists integers x and t such that:

$$ax + ny = 1 \tag{3.2.95}$$

If $1 \leq x < n$ and $(x, n) = 1, x \in S$. If not, then by division algorithm in integers there exist integers q and r such that:

$$x = qn + r, \qquad 0 \leq r < n \tag{3.2.96}$$

Now:

$$\begin{aligned} ax + ny &= 1 \\ \Rightarrow aqn + ar + ny &= 1 \\ \Rightarrow ar &= 1 + (-aq - y)n \end{aligned} \tag{3.2.97}$$

So $a * r = 1$. Similarly one can show that $r * a = 1$. Again if $(r, n) \neq 1$¡ , let p be a prime number dividing r and n. Then p will divide x. So p divides 1 as $ax + ny = 1$ which does not make sense. Therefore $(r, n) = 1$, hence $r \in S$. Therefore $\langle S, * \rangle$ is a group. It is easy to verify that S is abelian.

Example 18

Problem: Show that the set:

$$G = \{1, \omega, \omega^2\} \tag{3.2.98}$$

forms an abelian group under the usual multiplication operation, where $1, \omega, \omega^2$ are cube roots of 1.

Solution: The composition table is

	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

Table 37: Composition table for G

Closure⇒ Obviously holds from the composition table.
Identity⇒ 1 is the identity as the operation is multiplication.
Commutativity⇒ Obviously holds from the composition table.
Associativity⇒ Obviously holds from the composition table.

Therefore $\langle G, *\rangle$ is an abelian group.

Example 19

Problem: Show that the set of all 2×2 matrices over integers forms an abelian group w.r.t matrix addition.

Solution: Consider

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$a, b, c, d \in Z$. Clearly M is a non-empty set. Also $\forall A, B \in M$, $A + B$ is also a 2×2 matrix belonging to M, therefore closure holds. Since the primary operation is addition commutativity and associativity holds. Identity is just the matrix with elements being zero:

$$I = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

The inverse is also easy to see:

$$Inverse = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$$

Example 20

Problem: Prove that matrices:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

form a group under matrix multiplication.

Solution: Let G be the set containing the matrices. Consider:

$$IA = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = A$$

$$II = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$

$$AI = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = A$$

$$AA = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$

Which can be written as a composition table as:

	A	I
A	I	A
I	A	I

Table 38: Composition table for G

Closure ⇒ Obvious from table
Identity ⇒ I is the identity matrix (note that I is in-fact the identity matrix for any 2×2 matrix).
Inverse ⇒ $A \& I$ are each others' inverse, therefore are Hermitian matrices.
Associativity ⇒ We want to show:

$$A * (A * I) = (A * A) * I$$

Consider:

$$\begin{aligned} A*(A*I) &= A*A \\ &= I \end{aligned} \tag{3.2.109}$$

$$\begin{aligned} (A*A)*I &= I*I \\ &= I \end{aligned} \tag{3.2.110}$$

Associativity holds.
Commutativity $\Rightarrow A*I = I*A$, therefore commutativity holds.
Therefore the set G forms an abelian group under matrix multiplication. Note the similarity between the group $\{1, -2\}$ under multiplication operator. So A is analogous to -1 in this case and I is analogous to 1.

3.3 Power elements of groups

If $\langle G, \cdot \rangle$ is a group and $a \in G$, then we denote $a \cdot a$ by a^2 which is again a member of G. Similarly $a^3 = a^2 \cdot a$ and so on. One can show:

$$a^m a^n = a^{m+n} \tag{3.3.1}$$

$$(a^m)^n = a^{mn} \tag{3.3.2}$$

$$a^{-m} = (a^m)^{-1} \tag{3.3.3}$$

Example 21

Problem: If G is a group such that:

$$(ab)^2 = a^2b^2 \qquad \forall a, b \in G \tag{3.3.4}$$

show that G is abelian.

Solution: We are told that G is a group therefore the four properties are satisfied. We just need to check for commutativity. Consider:

$$\begin{aligned} (ab^2) &= a^2b^2 & \\ (ab)(ab) &= (aa)(bb) & \\ (aba)b &= (aab)b & \text{(Associativity)} \\ (aba) &= aab & \text{(Cancellation)} \\ ba &= ab & \end{aligned} \tag{3.3.5}$$

Therefore G is abelian.

Example 22

Problem: Prove if every element of a group G is its own inverse then G is abelian.

Solution: $\forall a, b \in G$

$$\begin{aligned} ab &= (ab)^{-1} \\ &= b^{-1}a^{-1} \qquad (3.3.6) \end{aligned}$$

But as $a, b \in G$ and we are given:

$$a^{-1} = a \qquad (3.3.7)$$

$$b^{-1} = b \qquad (3.3.8)$$

Therefore Eq 3.3.6 becomes:

$$ab = ba \qquad (3.3.9)$$

Hence G is abelian.

Example 23

Problem: Prove that a group G having three elements is always abelian.

Solution: Lets define the three elements as:

$$e, a, b \in G \qquad (3.3.10)$$

where e is the identity. Now:

$$ab \in G \qquad \text{(Closure)} \qquad (3.3.11)$$

Therefore:

$$ab = e \qquad (3.3.12)$$

or

$$ab = a \qquad (3.3.13)$$

or

$$ab = b \qquad (3.3.14)$$

First consider $ab = b$:

$$\begin{aligned} ab &= b \\ ab &= eb \qquad \text{(Cancellation law)} \\ a &= e \qquad (3.3.15) \end{aligned}$$

Which is obviously not true. Secondly:

$$\begin{aligned} ab &= a \\ ab &= ea \\ b &= e \qquad (3.3.16) \end{aligned}$$

which is not true. Therefore $ab = e$ must be true:

$$\begin{aligned} ea &= ae \\ eb &= be \\ ee &= ee \end{aligned} \tag{3.3.17}$$

and so each element commutes with all others, therefore G is abelian.

Example 24

Problem: Show that $\forall a, b \in G$ the equations:

$$ax = b \tag{3.3.18}$$
$$ya = b \tag{3.3.19}$$

have unique solutions $\forall x, y \in G$.

Solution: The solutions are:

$$x = ba^{-1} \tag{3.3.20}$$

Suppose there is another solution x_2 then we have the two equations:

$$\begin{aligned} ax &= b \\ ax_2 &= b \end{aligned}$$

Therefore:

$$\begin{aligned} ax &= ax_2 \\ x & \quad x_2 \end{aligned} \tag{3.3.21}$$

So the solution is indeed unique. One can do the same thing for $ya = b$.

3.4 Rings

Groups contain a non-empty set along with one binary composition. A system can be defined with a non-empty set with two binary compositions.

Definition: Let R be a non-empty set and '+' and '$\cdot$' be the two binary compositions on R. The R is said to form a ring w.r.t'+' and '$\cdot$' if the following properties are satisfied:

1)

$$a + b = b + a \qquad \forall\, a, b \in R \tag{3.4.1}$$

2)

$$a + (b + c) = (a + b) + c \qquad \forall\, a, b, c \in R \tag{3.4.2}$$

3)

$$\exists\, 0 \in R \tag{3.4.3}$$

Such that:

$$a + 0 = 0 + a = a \qquad \forall\, a \in R \tag{3.4.4}$$

4)

$$\forall\, a \in R, \exists(-a) \in R \tag{3.4.5}$$

Such that:

$$a(-a) = (-a) + a = 0 \tag{3.4.6}$$

5)

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \qquad \forall\, a, b, c \in R \tag{3.4.7}$$

6)

$$a \cdot (b + c) = a \cdot b + a \cdot c \qquad \forall\, a, b, c \in R \tag{3.4.8}$$

$$(b + c) \cdot a = b \cdot a + c \cdot a \tag{3.4.9}$$

Since + and $\cdot$ are binary operations defined on R, the closure properties must hold for each of them individually; i.e $\forall a, b \in R$:

$$a + b \in R \tag{3.4.10}$$

and

$$a \cdot b \in R \tag{3.4.11}$$

Axioms 1-4 are just showing that $\langle R, + \rangle$ forms an abelian group. Axiom 3 shows the identity requirement and once again the identity is unique. This is generally called the *zero* of the ring. The requirement of the zero requirement is sometimes called the additive identity of R.

3.5 Commutative ring

A ring R, with the property:

$$ab = ba \qquad \forall\, a, b \in R \tag{3.5.1}$$

is called a commutative ring.

3.6 Ring with unity

An element e of a ring R is called a the *unity* of R if:

$$ae = ea = a \qquad \forall\, a \in R \tag{3.6.1}$$

Any ring having unity is originally called a *ring with unity.* In general, a ring may or may not have a unity element, but if unity exists, it must be unique. Suppose there are two unities, e_1 and e_2:

$$ae_2 = e_2a = a \tag{3.6.2}$$

$$ae_1 = e_1 a = a \tag{3.6.3}$$

The proof follows (quite obviously) from the one given in the groups section for the uniqueness of the identity. In general, the unity of a ring R is denoted by 1.

Example 25

Problem: Check that$\langle R, +, \cdot$, where R is the set of all real numbers and $+$ and $\cdot$ are the usual addition and multiplication operators, forms a commutative ring with unity.

Solution: $\forall a, b \in R$:

$$a + b = b + a \tag{3.6.4}$$

Obviously holds for all real numbers. And the other axioms from 1 to 4 are satisfied. The real numbers 0 and 1 act as the zero and unity of this ring.

Example 26

Problem: Check weather $\langle Z, +, \cdot\rangle$ where Z is the set of integers and $+$ and $\cdot$ are the usual addition and multiplication operators, forms a commutative ring with unity.

Solution: Axioms 1 to 4 are satisfied as $\langle Z, +\rangle$ forms an abelian group. The zero is 0 and the unity is 1 for this ring.

Example 27

Problem: Let E be the set of all even integers. Show that E forms a commutative ring *without* unity, under usual addition and multiplication operators.

Solution: Since the sum and product of any two even integers is again an even integer we note that $+$ and $\cdot$ are well defined binary operations on E. It is, of course, very to prove other properties. Note that since there does not exist any even integer such that:

$$ex = xe = x \qquad \forall\, x \in E \tag{3.6.5}$$

E is a ring without unity.

Example 28

Problem: The set M of all 2×2 matrices over integers forms a non-commutative ring w.r.t matrix addition and multiplication.

Solution: When discussing groups, it was observed that M forms an abelian group w.r.t matrix addition, therefore axioms 1 to 4 are satisfied. Matrix multiplication is associative and distributive, therefore M is a ring. The unity is the identity matrix:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

The commutation for the multiplication equation does not hold. Consider two matrices A and B:

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}$$

$$B = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$$

The product AB is:

$$AB = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 3 & 0 \end{pmatrix}$$

and BA is:

$$BA = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$$

So we see $AB \neq BA$. Hence M forms a non-commuting ring with unity.

Example 29

Problem: Let G be an additive abelian group with at least two elements. Define a binary composition on G by:

$$x \cdot y = 0 \qquad \forall x, y \in G \tag{3.6.11}$$

Show that $\langle G, +, \cdot \rangle$ is a commutative ring without unity.

Solution: It is already given that $\langle G, + \rangle$ is an abelian group. So we need to prove only axioms 5&6:

$$\begin{aligned} a \cdot (b \cdot c) &= a \cdot 0 \\ &= 0 \end{aligned} \tag{3.6.12}$$

$$\begin{aligned} (a \cdot b) \cdot c &= 0 \cdot c \\ &= 0 \end{aligned} \tag{3.6.13}$$

$$\Rightarrow \qquad a \cdot (b \cdot c) = (a \cdot b) \cdot c \tag{3.6.14}$$

Also:

$$\begin{aligned} a \cdot (b + c) &= 0 \\ a \cdot b + a \cdot c &= 0 + 0 = 0 \\ a \cdot (b + c) &= a \cdot b + a \cdot c \end{aligned} \tag{3.6.15}$$

Similarly:

$$(b + c) \cdot a = b \cdot a + c \cdot a \tag{3.6.16}$$

Thus $\langle G, +, \cdot \rangle$ is a ring. Clearly:

$$a \cdot b = 0 = b \cdot a \qquad \forall a, b \in G \tag{3.6.17}$$

Therefore G is commutative. There does not exist any element $e \in G$ such that:

$$a \cdot e = e \cdot a = a \qquad \forall a \in G \tag{3.6.18}$$

as:

$$e \cdot a = 0 \qquad \forall a, e \in G \tag{3.6.19}$$

Therefore G is without unity.

Example 30

Problem: Define

$$R = \{0, 1, 2, 4, 5, 6\} \tag{3.6.20}$$

and let $\oplus$ and $\odot$ be the addition and multiplication modulo 7 respectively. Show that $\langle R, \oplus, \odot$ forms a ring.

Solution: In the groups section it is show that $\oplus$ and $\odot$ are binary operators on R. It has already been shown that $\langle R, \oplus \rangle$ forms an abelian group. It has also been proved that:

$$a \odot (b \odot c) = (a \odot b) \odot c \tag{3.6.21}$$

Consider:

$$2 \odot (2 \oplus 4) = 2 \odot 0 = 0 \tag{3.6.22}$$

$$2 \odot 3 \oplus 2 \odot 4 = 6 \oplus 1 = 0 \tag{3.6.23}$$

$$\Rightarrow 2 \odot (3 \oplus 4) = 2 \odot 3 \oplus 2 \odot 4 \tag{3.6.24}$$

The result would be true $\forall a, b, c \in R$, therefore $\langle R, \oplus, \odot \rangle$ is a ring.

Example 31

Problem: Let $R = \{(a, b) | a, b \text{are rational numbers}\}$. Define $\oplus$ and $\odot$ by:

$$(a,b) \oplus (c,d) = (a+c, b+d) \tag{3.6.25}$$

$$(a,b) \odot (c,d) = (ac, bd) \tag{3.6.26}$$

Show that $\langle R, \oplus, \odot \rangle$ forms a commutative ring with unity.

Solution: By the definitions $\oplus$ and $\odot$ are binary operators, $\oplus$ is commutative:

$$\begin{aligned} (a,b) \oplus (c,d) &= (a+c, b+d) \\ &= (c+a, d+b) \\ &= (c,d) \oplus (a,b) \end{aligned} \tag{3.6.27}$$

$\oplus$ is associative.
Identity $\Rightarrow$:

$$\begin{aligned} (a,b) \oplus (0,0) &= (a+0, b+0) \\ &= (a,b) \qquad\qquad \forall\ (a,b) \in R \end{aligned} \tag{3.6.28}$$

So the identity is (0,0).
Inverse $\Rightarrow \forall (a,b) \in R, \exists\ (-a,-b) \in R$ such that:

$$(a,b) \oplus (-a,-b) = (a-a, b-b) = (0,0) \tag{3.6.29}$$

Therefore $(-a,-b)$ is the inverse of $(a,b) \forall a, b$.
Associativity$\Rightarrow$

$$\begin{aligned} [(a,b) \odot (c,d)] \odot (e,f) &= (ac, bd) \odot (e,f) \\ &= ace, bdf \end{aligned} \tag{3.6.30}$$

Therefore $\odot$ is associative.
Distributive $\Rightarrow$:

$$\begin{aligned} (a,b) \odot [(c,d) + (e,f)] &= (a,b) \odot (c+e, d+f) \\ &= [a(c+e), b(d+f)] \\ &= (ac+ae, bd+bf) \end{aligned} \tag{3.6.31}$$

$$\begin{aligned} (a,b) \odot (c,d) \oplus (a,b) \odot (e,f) &= (ac,bd) \oplus (ae,bf) \\ &= (ac+ae, bd+bf) \end{aligned} \tag{3.6.32}$$

Therefore distributivity holds. Hence $\langle R, \oplus, \odot \rangle$ is a ring.
Commutativity $\Rightarrow$

$$\begin{aligned} (a,b) \odot (c,d) &= (ac, bd) \\ &= (ca, db) \\ &= (c,d) \odot (a,b) \end{aligned} \tag{3.6.33}$$

Therefore R is commutative.
Unity ⇒

$$\begin{aligned} (a,b)\odot(1,1) &= (a\cdot 1, b\cdot 1) \\ &= (a,b) \\ &= (1,1)\odot(a,b) \qquad \forall a,b\in R \end{aligned} \tag{3.6.34}$$

Therefore R is a commutative ring with unity.

3.6.1 Properties

Suppose $\langle R,+,\cdot\rangle$ is a ring and $a,b,c\in R$ are any members:

1)

$$a\cdot 0 = 0\cdot a = 0 \tag{3.6.35}$$

Proof:

$$\begin{aligned} a\cdot 0 &= a\cdot(0+0) \\ &= a\cdot 0 + a\cdot 0 \\ \Rightarrow\ a\cdot 0+(-a\cdot 0) &= (a\cdot 0+a\cdot 0)+(-a\cdot 0) \\ &= a\cdot 0+[a\cdot 0+(-a\cdot 0)] \\ &= a\cdot 0+0 \\ \Rightarrow 0 &= a\cdot 0+0 \\ &= a\cdot 0 \end{aligned} \tag{3.6.36}$$

Similarly $0\cdot a = 0$.

Therefore 0 is the zero (additive identity) and (-a) is the inverse of a.

2)

$$a\cdot(b-c)+a\cdot c = a\cdot b - a\cdot c \tag{3.6.37}$$

Proof:

$$\begin{aligned} a\cdot(b-c)+a\cdot c &= a\cdot[(b-c)+c] \\ &= a\cdot[b+(-c+c)] \\ &= a\cdot[b+0] \\ &= a\cdot b \end{aligned} \tag{3.6.38}$$

$$\Rightarrow a\cdot(b-c)+a\cdot c+(-a\cdot c) = a\cdot b - a\cdot c \tag{3.6.39}$$

$$\Rightarrow a\cdot(b-c)+0 = a\cdot b - a\cdot c \tag{3.6.40}$$

$$\Rightarrow a\cdot(b-c)+a\cdot b - a\cdot c \tag{3.6.41}$$

3)

$$-(-a) = a \tag{3.6.42}$$

Proof: Let b be the additive inverse of $-a$:

$$b = -(-a) \tag{3.6.43}$$

then

$$b + (-a) = 0 \tag{3.6.44}$$

$$\Rightarrow b + (-a) + a = 0 + a \tag{3.6.45}$$

$$\Rightarrow b + 0 = a \tag{3.6.46}$$

$$\Rightarrow b = a \tag{3.6.47}$$

$$-(-a) = a \tag{3.6.48}$$

4)

$$a \cdot (-b) = (-a) \cdot b = -a \cdot b \tag{3.6.49}$$

Proof:

$$\begin{aligned} a \cdot (-b) &= a \cdot (0 - b) \\ &= a \cdot 0 - a \cdot b \\ &= 0 - a \cdot b \end{aligned} \tag{3.6.50}$$

Similarly:

$$(-a) \cdot b = -a \cdot b \tag{3.6.51}$$

5) :

$$(-a) \cdot (-b) = a \cdot b \tag{3.6.52}$$

Proof:

$$\begin{aligned} (-a) \cdot (-b) &= -[a \cdot (-b)] \\ &= -[-a \cdot b] \\ &= a \cdot b \end{aligned} \tag{3.6.53}$$

Example 32

Problem: Show that a ring $\langle R, +, \cdot \rangle$ is commutative if and only of:

$$(a + b)^2 = a^2 + 2ab + b^2 \qquad \forall a, b \in R \tag{3.6.54}$$

where $a^2 = a \cdot a$.

Solution:

$$(a+b)^2 = a^2 + ab + ba + b^2 \tag{3.6.55}$$

we are told:

$$(a+b)^2 = a^2 + 2ab + b^2 \tag{3.6.56}$$

Therefore:

$$\begin{aligned} a^2 + ab + ba + b^2 &= a^2 + 2ab + b^2 \\ ab + ba &= 2ab \\ ab &= ba \end{aligned} \tag{3.6.57}$$

Example 39

Problem: If $x \in R$ and $x^2 = x$, prove that R must be commutative.

Solution: Let $a, b \in R$:

$$\begin{aligned} (a+b)^2 &= a = b \qquad \text{as } x^2 = x \\ a^2 + ab + ba + b^2 &= a + b \end{aligned} \tag{3.6.58}$$

We are given:

$$a^2 = a \tag{3.6.59}$$

$$b^2 = b \tag{3.6.60}$$

Therefore:

$$\begin{aligned} a^2 + ab + ba + b^2 &= a + b + ab + ba \\ a + b + ab + ba &= a + b \\ ab + ba &= 0 \\ ab &= -ba = (-b)a \end{aligned} \tag{3.6.61}$$

Now:

$$\begin{aligned} (-b) &= (-b)^2 \\ &= (-b)(-b) \\ &= b^2 \\ &= b \end{aligned} \tag{3.6.62}$$

Therefore $ab = ba$.

Example 34

Problem: If $\langle R, +, \cdot \rangle$ is a system satisfying all axioms of a ring with unity, except that $a + b = b + a$, shows that this axiom also holds.

Solution: It is given that $1 \in R$, therefore $1 + 1 \in R$:

$$\begin{aligned} (a+b)(1+1) &= a(1+1) + b(1+1) \\ &= a + a + b + b \end{aligned} \tag{3.6.63}$$

Also:

$$\begin{aligned} (a+b)(1+1) &= (a+b)1 + (a+b)a \\ &= a + b + a + b \\ \Rightarrow a + a + b + b &= a + b + a + b \\ \Rightarrow a + b &= b + a \end{aligned} \tag{3.6.64}$$

3.7 Integral Domain

If R is a commutative ring, then $0 \neq a \in R$ is said to be a zero divisor if $\exists\, b \in R, b \neq 0$, such that $ab = 0$. Or more concisely:

$$ab = 0 \qquad \forall\, a, b \in R \quad \text{where } a, b \neq 0 \tag{3.7.1}$$

A commutative ring R is called an *integral domain* if it has no zero divisors i.e a commutative ring R is called an integral domain if:

$$ab = 0 \tag{3.7.2}$$

If $a = 0$ or $b = 0$. The ring $\langle Z, +, \cdot \rangle$ of integers is an integral domain.

Example 35

Problem: Give an example of a commutative ring, which is not an integral domain.

Solution: Define:

$$R = \{0, 1, 2, 3, 4, 5\} \tag{3.7.3}$$

The operations $\oplus$ and $\odot$ are the addition and multiplication modulo 6. It forms a commutative ring (look at Example 30. Note that:

$$2 \odot 3 = 0 \tag{3.7.4}$$

and $2, 3 \neq 0$. Therefore $\exists a, b \in R$ such that $ab = 0$, where as $a, b \neq 0$. Hence it is not an integral domain. On the other hand if $\odot$ and $\oplus$ stand for the multiplication and addition modulo 5, then R is an integral domain as:

$$0 \oplus 5 = 0 \tag{3.7.5}$$

3.8 Fields

A non-empty set, F, together with two binary operations + and $\cdot$ is said to form a *field* if $\forall a, b, c \in F$:

1)

$$a + (b + c) = (a + b) + c \tag{3.8.1}$$

2)

$$a + b = b + a \tag{3.8.2}$$

3) $\exists 0 \in F$ such that:

$$a + 0 = 0 + a = a \tag{3.8.3}$$

4) $\forall a \in F, \exists - a \in F$ such that:

$$a + (-a) = (-a) + a = 0 \tag{3.8.4}$$

5)

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \tag{3.8.5}$$

6)

$$a \cdot b = b \cdot a \tag{3.8.6}$$

7) $\exists | \in F$ such that

$$a \cdot 1 = a \cdot 1 = a \tag{3.8.7}$$

8) $\forall a \in F, \exists a^{-1} \in F$ where $a \neq 0$ such that:

$$a \cdot a^{-1} = a^{-1} \cdot a = 1 \tag{3.8.8}$$

9)

$$a \cdot (b + c) = a \cdot b + a \cdot c \tag{3.8.9}$$

$$(b + c) \cdot a = b \cdot a + c \cdot a \tag{3.8.10}$$

In short, a field is a commutative ring with unity in which non-zero elements have a multiplication inverse (i,e both the operations have an inverse element associated with them). A ring with unity is said to be a division ring if its non zero elements have a multiplicative inverse, therefore a field is the same as a commutative division ring. One could also say a ring with unity is a division ring if its non-zero elements, forms a group w.r.t multiplication.

Example 36

The set R, of real numbers forms a field under the usual addition and multiplication (Proof is obvious).

Example 37

The set Q of all rational numbers forms a field under addition and multiplication (Proof is obvious).

Example 38

Problem: Check the set:

$$R = \{0, 1, 2, 3, 4, 5, 6\} \tag{3.8.11}$$

forms a field under the multiplication and addition modulo of 7.

Solution: It was previously shown that $\langle R, \oplus, \odot \rangle$ forms a commutative ring. 1 is the unity of this ring. Since:

$$\begin{aligned} 1 \odot 1 &= 1 = 6 \odot 6 \\ 2 \odot 3 &= 1 = 4 \odot 2 \\ 3 \odot 5 &= 1 = 5 \odot 3 \end{aligned}$$

So the non zero elements have multiplicative inverse; 1 is inverse of 1, 2 of 4, 3 of 5.

Example 39

Problem: Show that the set:

$$F = \{a + b\sqrt{2} | a, b \text{are rational numbers}\} \tag{3.8.12}$$

is a field under usual addition and multiplication.

Solution: Closure for addition:

$$a + b\sqrt{2}, c + d\sqrt{2} \in F \tag{3.8.13}$$

Now:

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \tag{3.8.14}$$

Also $\in F$ as $(a + c)$ and $(b + d)$ are rationals.

Closure for multiplication:

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in F \tag{3.8.15}$$

as $ac + 2bd$ and $ad + bc$ are rationals.

Associativity for addition:

$$\begin{aligned}[(a+b\sqrt{2})+(c+d\sqrt{2})]+(e+f\sqrt{2}) &= (a+c)+(b+d)\sqrt{2}+e+f\sqrt{2} \\ &= (a+c+e)+(b+d+f)\sqrt{2} \\ &= (a+b\sqrt{2})+(c+e)+(d+f)\sqrt{2} \\ &= (a+b\sqrt{2})+[(c+d\sqrt{2})+(e+f\sqrt{2})]\end{aligned} \tag{3.8.16}$$

Identity for addition:

$$0+0\sqrt{2}\in F \tag{3.8.17}$$

and

$$\begin{aligned}(a+b\sqrt{2})+(0+0\sqrt{2}) &= (a+0)+(b+0)\sqrt{2} \\ &= 0+0\sqrt{2}\end{aligned} \tag{3.8.18}$$

Therefore $0+0\sqrt{2}$ is the additive identity.

Inverse of addition; $\forall a+b\sqrt{2}\in F$, $\exists, -a-b\sqrt{2}\in F$ such that:

$$\begin{aligned}(a+b\sqrt{2})+(-a-b\sqrt{2}) &= (a-a)+(b-b)\sqrt{2} \\ &= 0+0\sqrt{2}\end{aligned} \tag{3.8.19}$$

Therefore $-a-b\sqrt{2}$ is inverse of $a+b\sqrt{2}$. Associativity and commutativity are obvious to prove.

Distributivity:

$$\begin{aligned}(a+b\sqrt{2})[(c+d\sqrt{2})+(e+f\sqrt{2})] &= (a+b\sqrt{2})[(c+e)+(d+f)\sqrt{2}] \\ &= [ac+ae+2(bd+fb)]+(ad+af+bc+be)\sqrt{2} \\ &= [(ac+2bd)+(ad+bc)\sqrt{2}]+[(ae+2bf)+(af+be)\sqrt{2}] \\ &= (a+b\sqrt{2})(c+d\sqrt{2})+(a+b\sqrt{2})(e+f\sqrt{2})\end{aligned} \tag{3.8.20}$$

Similarly right distributivity can be verified.

Unity is $1+0\sqrt{2}\in F$.

Inverse of multiplicity:

$$\begin{aligned}\frac{1}{a+b\sqrt{2}} &= \frac{1}{a+b\sqrt{2}}\times\frac{a-b\sqrt{2}}{a-b\sqrt{2}} \\ &= \frac{a-b\sqrt{2}}{a^2-2b^2} \\ &= \frac{a}{a^2-2^2}+\frac{-b}{a^2-2b^2}\sqrt{2}\end{aligned} \tag{3.8.21}$$

Which is also in F. Since:

$$a + b\sqrt{2} \times \frac{1}{a + b\sqrt{2}} = 1 \tag{3.8.22}$$

Therefore:

$$(a + b\sqrt{2}) \times \frac{a}{a^2 - 2^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2} = 1 \tag{3.8.23}$$

Therefore $\frac{a}{a^2-2^2} + \frac{-b}{a^2-2b^2}\sqrt{2}$ is the inverse. Hence F is a field.

3.8.1 Equality between fields and integral domain

Let $\langle F, +, \cdot \rangle$ be a field. We show that F has no zero divisors. Suppose, F has zero divisors $\exists a, b \in F$ $(a, b \neq 0)$, such that $ab = 0$:

$$\Rightarrow a^{-1}(ab) = a^{-1} = 0 \tag{3.8.24}$$

a^{-1} is the inverse (multiplicity inverse) of a:

$$\begin{aligned} \Rightarrow (a^{-1}a)b &= 0 \\ b &= 0 \end{aligned} \tag{3.8.25}$$

This is a contradiction as $b \neq 0$ was first defined. This means F has no zero divisors and hence it is an integral domain. A field is always an integral domain, but an integral domain is *not* always a field. For example a set of integers forms an integral domain but not a field. It is provable that any *finite* integral domain is a field.