2. Groups

2.1 The defnition of a Group

A group G(*) is a set G of elements with a binary operation * defined upon it such that

i) G is closed with respect to *

ii) $(a*b)*c = a*(b*c) \quad \forall\ a, b$ and $c \in$ G (associative law)

iii) G contains an *identity* element e such that $a*e = e*a = a \quad \forall$ a $\in$ G

iv) to each element $a \in$ G there corresponds an *inverse* $\bar{a} \in$ G such that $a * \bar{a} = \bar{a} * a = e$

In addition if the binary operation is commutative we say the group is Abelian.

The groups that we meet on this course divide into finite groups and infinite groups. We will first look at some examples of infinite groups.

2.2 Infinite Groups

To establish if a binary operation defined on a set forms a group we need to establish if the 4 group axioms hold. Many of the examples that follow will be obvious as they involve binary operations with which we are familiar.

Example2.2.1

Z(+) (the set of integers with the binary operation addition)

$a + b \in \mathbf{Z}, \quad \forall\ a, b \in \mathbf{Z},$ so **Z** is closed w.r.t. +

+ of integers is associative

$a + 0 = 0 + a = a, \quad \forall\ a \in \mathbf{Z}$ so 0 is the *identity*

$a + (-a) = (-a) + a = 0 \quad \forall\ a \in \mathbf{Z}$ so $-a$ is the inverse of a

Hence **Z**(+) is a group

Example2.2.2

Z(–) (the set of integers with the binary operation subtraction)

$(a - b) - c \neq a - (b - c)$ ie subtraction of integers is not associative

Hence **Z**(–) is not a group

Example2.2.3

Z(.) (the set of integers with the binary operation multiplication)

$ab \in \mathbf{Z}, \quad \forall\ a, b \in \mathbf{Z},$ so **Z** is closed w.r.t. multiplication

$a.1 = 1.\ a = a, \quad \forall\ a \in \mathbf{Z}$ so 1 is the *identity*

$a.\ 1/a = 1/a\ .\ a = 1$ so $1/a$ is the inverse of a BUT $1/a \notin \mathbf{Z}$

Hence **Z**(.) is a not group

Exercise 2.2

1. Which of the following sets form groups under the operations $+, -, \times$ or $\div$?

   Things to think about: a) well-defined? b) closed? c) associative? d) commutative? e) identity? f) inverses?

	$+$	$-$	$\times$	$\div$
N				
Z				
Q				
Q – {0}				
R				
R – {0}				
m × n matrices				
n × n matrices				
n × n non-sing. matrices				

2. Which of the following sets form a group w.r.t. the given operation.

   a) $\{a : a \in \mathbf{Z} \text{ and } a < 0\}$ addition;
   b) $\{5a : a \in \mathbf{Z}\}$ addition;
   c) $\{a : a \in \mathbf{Z} \text{ and } a \text{ is odd}\}$ multiplication;
   d) $\{z : z \in \mathbf{C} \text{ and } |z| = 1\}$ multiplication
   e) The set of all polynomials in x of degree ≤ 3 w.r.t. addition;
   f) The same set as e) w.r.t. multiplication;
   g) The set of all polynomials in x of degree ≥ 3 w.r.t. addition.

2.3 Finite Groups

When considering a small set and a binary operation it is often possible to draw up a structure table which gives the results of combining all possible pairs of elements and enables us to quickly establish whether the closure, identity and inverse axioms apply. A structure table will **not** tell us anything about associativity.

Associativity may be obvious from the nature of the binary operation. If it is not obvious it ought to be established for all possible cases - this can be extremely tedious. In this unit you will not be given examples where it is necessary to do this from a structure table.

Example 2.3.1

Consider the set $\{ 1, -1, i, -i \}$ w.r.t. multiplication where $i^2 = -1$

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

By observing the table we can see that

i) the operation is closed as only the set elements appear in the table

ii) 1 is the identity.

iii) each element has an inverse, ie $1 \times 1 = 1$, $-1 \times -1 = 1$ (we say these are self inverse) and $i \times -i = 1$ and $-i \times i = 1$, ie $-i$ is the inverse of i, and i is the inverse of $-i$

Also regarding $\{ 1, -1, i, -i \}$as a subset of **C**, we know that multiplication is associative. Hence the 4 axioms are satisfied so we have a group

There are one or two simple conventions we adopt when drawing up a table like the one above.

- the identity always appears first, both across and down
- the order in which the elements appear is the same across and down
- to find $a*b$ we look in row a and column b

Exercise 2.3

Complete structure tables for the following sets and associated binary operations, checking from the whether the closure , identity and inverse axioms apply.

	Set	Binary Operation
1.	$\{1, -1\}$	multiplication
2.	$\{1, \omega, \omega^2\}$ where $\omega^3 = 1$	multiplication

3.	$\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \}$	matrix multiplication (*Hint you may find it easier to give the matrices names like* I, A, B, C)
4.	$\{ 1, r, r^2, r^3, r^4, r^5 \}$, where r represents a rotation of 60°, and r^2 is a rotation of 120°	composition of rotations, ie one rotation followed by another.
5.	{ (0,0,0,0), (1,1,0,1), (0,0,1,1), (1,1,1,0) }	binary addition of digits