Introduction To Group Theory

The everyday concept of **groups** which simply means an assemblage of persons or things, is familiar to most people . *Group* in the mathematical sense, is defined more strictly. In addition to its basic definition, it must meet certain criteria. One of the mathematical purpose of group theory is to establish an algebraic structure within which algebraic thoughts can be manipulated.

Definitions

Binary operation: a rule that combine two elements (**operands**) in order to produce another element. There are several symbols used for specific binary operations. However, the symbol o is a common symbol used to indicate an arbitrary binary operation.

Set: a collections of objects. For example, the set of countries in the Africa; the set of politicians who are statesmen; the set of viable democracies in the world; etc. The objects belonging to the set are its *members* or *elements.*

Now let G be a set and o a binary operation defined on G. Then the criteria that establish (G, o) as a **group** are as follows:

Closure: for all g_1 and g_2 ∈ G, g_1 o g_2 ∈ G. In other words, take two elements from the set G and perform a binary operation on them. The result must be an element of G.

I**dentity**: there is an *identity element, e* ∈ G such that for all g ∈ G, g o *e* = g = *e* o g. The identity element is unique.

Inverses: there is an *inverse element*, g^{-1} ∈ G such that for all g ∈ G, g o g^{-1} = *e* = g^{-1} o g. Each element has a unique inverse and $(g^{-1})^{-1}$ = g.

Associativity: for all g_1, g_2, g_3, ∈ G, g_1 o (g_2 o g_3) = (g_1 o g_2) o g_3.

The *closure*, *identity*, *inverses* and *associativity* criteria (CIIA) establish a mathematical group. If the commutative criterion is included, then the group is called a **commutative group** or A**belian group**.

Commutativity: for all g_1, g_2 ∈ G, g_1 o g_2 = g_2 o g_1. (CIIAC) is an acronym for the criteria for a commutative group.

(1) Show that the (Z, +) is a group. Where Z is the set of integers and + is the binary operation of addition.

Ans (1) We need to show that each of the CIIA criteria is satisfied.
Closure is satisfied since for any x, y in Z, x + y is in Z
The identity element is 0. For any x in Z, x + 0 = x
The inverse element is -x. For any element in Z, x + – x = 0
Associativity is satisfied since for any x, y in Z, x + y = y + x.
So, (Z, +) is a group.

(R, +) is also a group by similar reasoning. Where R is the set of real numbers and + is the binary operation of addition.

(2) Show that (R^+, x) is a group. Where R^+ is the set of positive real numbers and x is the binary operation of multiplication.

Introduction To Group Theory

Ans (2) Closure is satisfied since for any u, v in R+, u x v is in R+
The identity element is 1. For any u in R+, u x 1 = u
The inverse element is u^{-1}. For any element in R+, u x u^{-1} = 1
Associativity is satisfied since for any u, v in R+, u x v = v x u.
So, (R+, x) is a group.

(3) Show that the set of all 2 x 2 matrices with non-zero determinants is a group.

Ans (3) Let **A** = (a_{11}, a_{12}, a_{21}, a_{22}) be an arbitrary 2 x 2 matrix. Where a_{ij} is the element in the i^{th} row and j^{th} column. The identity matrix is **I** = (a_{11}=1, a_{12}=0, a_{21}=0, a_{22}=1) and the inverse matrix is $\mathbf{A}^{-1}$ such that $\mathbf{AA}^{-1} = \mathbf{A}^{-1}\mathbf{A} = \mathbf{I}$. The closure and associative criteria are satisfied.

Some other familiar groups are:
- The set of all translation of the plane R^2
- The set of all rotations and translation of the plane and their composites
- The set of all composites of all reflections of the plane (isometry group of the plane).

Subgroup: (H, o) is a subgroup of (G, o) with identity *e*, if the CIIA criteria are satisfied with respect to H and *e* is also the identity element of (H, o).

(H, o) is a **normal subgroup** of (G, o) if for each element g Є G, gH = Hg.
Where gH = g o h (**left coset**) and Hg = h o g (**right coset**); h Є H.
Every subgroup of a **commutative** group (G, o) is a normal subgroup of (G, o).

The **order** of an element g of (G, o) is the least positive integer such that $g^n = e$. Non-existence of such integer implies g has **infinite order**.
A group is **cyclic** if every element of (G, o) is of the form g^n for some fixed g Є (G, o); g is called the **generator** of (G, o).
The **order** of a group is the number of element in it. A group is of **infinite order** if its elements are infinite.

Two groups (G, o) and (H,*) are **isomorphic** if there exists a mapping *f* : (G, o) → (H, *) such that the following criteria are met:
- *f* is one-one and onto
- $f(g_1 \circ g_2) = f(g_1 * g_2)$ for all g_1 , g_2 Є G.

The mapping *f*, is an **isomorphism**.

Peter Oye Simate Sagay
Simate was my mother
Sagay was my father