Groups-Introduction

Dear learners, in this module we are going to see about groups.

The modern treatment of abstract algebra begins with the simple abstract definition of a group. This simple definition quickly leads to difficult questions involving the structure of such objects. The term group was coined by Galois about 170 years ago to describe sets of one-to-one functions on finite sets that could be grouped together to form a closed set.

Binary Operation:
Let G be a set. A binary operation on G is a function that assigns each ordered pair of elements of G an element of G.

Group:
A Group G is a non-empty set together with a operation $*$ which satisfies the four properties:

Property 1.Closure: For a, b in G, $a * b$ is also in G.

Property 2.Associativity: $(a * b) * c = a * (b * c)$ for all a, b, c are in G.

Property 3.Identity: For all elements a in G,there is an element e (called the identity) in G, such that $a * e = e * a = a$.

Property 4.Inverse: For each element a in G, there is an element a^{-1} in G (called an inverse of a) such that $a * a^{-1} = a^{-1} * a = e$. That is the inverse of an element, combined with that element, gives the identity.

Property 5.Commutative: If a group has the property that $a * b = b * a$ for every pair of elements a and b, then the group is Abelian.

Semi-Group:
A non-empty set S with an operation $*$ is said to be a semi-group if it satisfies the Closure property and Associative property.

Monoid:
A non-empty set M with an operation $*$ is said to be a monoid if it satisfies the Closure property, Associative property and Identity property.

As in the case with most fundamental concepts in mathematics, the modern definition of a group that follows is the result of a long process. A set is a collection of well defined objects. An operation is a function that acts on two elements and results with a single element. For example $+, -, \times, \div$ are the operations on number system.
In 1890, Camille Jordan introduced the term Abelian group to honor Niels Henrik Abel, one of the foremost mathematicians of the nineteenth century.

A group is non-Abelian if there is some pair of elements a and b for which $a * b \neq b * a$.

Example:
Consider the set of integers $\mathbb{Z}$ with the operation usual addition $+$.

Property 1: Sum of any two integers is again an integer. Therefore closer property is true.

Property 2:Clearly $(a + b) + c = a + (b + c)$ for all integers a, b, c.Thus Associativity property is true.

Property 3:Clearly $a + 0 = 0 + a = a$ for all integer a. So the integer 0 plays the identity role.

Property 4:For each integer a in $\mathbb{Z}$, there is an integer $-a$ in $\mathbb{Z}$ such that $a + (-a) = -a + a = 0$.

Property 5: $a + b = b + a$ for all integers a and b. There the set of integers $\mathbb{Z}$ under addition $+$ is an Abelian group.
Hence the set of integers $\mathbb{Z}$ under addition $+$ is an abelian group.

Example:
The set of integers $\mathbb{Z}$ with the operation usual subtraction $-$.

Property 1:Subtraction of any two integers is again an integer. Therefore closer property is true.

Property 2: In general $(a - b) - c$ need not be equal to $a - (b - c)$ for integers a, b, c. For instance $(2 - 3) - 4 = -5$ whereas $2 - (3 - 4) = 3$. Thus Associativity property is not true.

Hence the set of integers $\mathbb{Z}$ under subtraction $-$ is not a group.

Example:
Consider the set of non-zero integers$\mathbb{Z}^*$with the operation multiplication $\times$.

Property 1: Product of any two non-zero integers is again a non-zero integer. Therefore closer property is true.

Property 2: Clearly $(a \times b) \times c = a \times (b \times c)$ for all non-zero integers a, b, c. Thus Associativity property is true.

Property 3:Clearly $a \times 1 = 1 \times a = a$ for all non-zero integer a. So the integer 1 plays the identity role in integer multiplication.

Property 4: For each non-zero integer $a \neq 1$, there is no non-zero integer b such that $a \times b = b \times a = 1$. For instance, $5 \times b \neq 1$ for any non-zero integer b. Thus Inverse property is not hold.

Hence the set of integers $\mathbb{Z}$ under multiplication $\times$ is not a group.

Example:
Consider the set of non-zero integers$\mathbb{Z}^*$with the operation multiplication $\div$.

Property 1: Division of any two non-zero integers is not an integer. Therefore$(\mathbb{Z}^*,\div)$ is not even binary.

Example:
Consider the set of integers $\mathbb{R}$ with the operation usual addition $+$.

Property 1: Sum of any two real number is again an real number. Therefore closer property is true.

Property 2: Clearly $(a+b)+c=a+(b+c)$ for all $a,b,c\in\mathbb{R}$. Thus Associativity property is true.

Property 3: Clearly $a+0=0+a=a$ for all $a\in\mathbb{R}$.Sothe integer 0 plays the identity role.

Property 4: For each integer a in $\mathbb{R}$, there is an integer $-a$ in $\mathbb{R}$ such that $a+(-a)=-a+a=0$.

Property 5: $a+b=b+a$ for all $a,b\in\mathbb{R}$.
Hence the set of reals $\mathbb{R}$ under addition $+$ is an abelian group.

Example:
Consider the set of non-zero integers$\mathbb{R}^*$with the operation multiplication $\times$.

Property 1: Product of any two non-zero reals is again a non-zero reals. Therefore closure property is true.

Property 2: Clearly $(a\times b)\times c=a\times(b\times c)$ for all $a,b,c\in\mathbb{R}^*$. Thus Associativity property is true.

Property 3: Clearly $a\times 1=1\times a=a$ for all $a\in\mathbb{R}^*$.So 1 plays the identity role in multiplication.

Property 4: For each $a\neq 1\in\mathbb{R}$, there is a non-zero $b\in\mathbb{R}^*$such that $a\times b=b\times a=1$. Thus Inverse property is hold.

Property 5: $a\times b=b\times a$ for all $a,b\in\mathbb{R}$.
Hence $(\mathbb{R}^*,\times)$is an abelian group.

Cayley table is an effective tool to find whether a finite set together with an operations is a group of not. A Cayley table describes the structure of a finite group by arranging all the group elements in a square table. It is named after the 19th century British Mathematician Authur Cayley.

Example:
Consider the set all cubic root of unity $G = \{1, \omega, \omega^2\}$ under multiplication.

$\times$	1	ω	ω^2
1	1	ω	ω^2
Ω	ω	ω^2	1
ω^2	ω^2	1	ω

Then it is clear from the Cayley Table that $\mathbf{G}$ is Closer, Associativity, Commutative and the Identity is 1.Further the inverse of 1 is 1.The inverse of ω is $\boldsymbol{\omega^2}$**.** And the inverse of $\omega^2$is ω. Therefore$(G,\times)$ is an abelian group.
In general $(G = \{1, \omega, \omega^2, \dots, \omega^3\},\times)$ is an abelian group.

Example:
Consider the Cayley Table for the set of integer modulo 4,$\mathbb{Z}_4$.

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Then it is clear from the Cayley Table that $\mathbb{Z}_4$ is Closer, Associativity, Commutative and the Identity is 0. Further the inverse of 0 is 0 the inverse of 1 is 3, the inverse of 2 is 2 . And the inverse of 3 is 1. Therefore $(\mathbb{Z}, +)$ is an abelian group.
In general $(\mathbb{Z}_n = \{0,1,2, \dots, n-1\}, +)$ is an abelian group.

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Similarly, it is clear from the Cayley Table that $\mathbb{Z}_4$ is Closer, Associativity, Commutative and the Identity is 1.Further the inverse of 1 is 1 the inverse of 3 is 3, the inverse of 2 does not exist. Therefore $(\mathbb{Z},\times)$ is not even a group.

Example:
Consider the set of all complex number $\mathbb{C}$ under complex addition $+$.

Property 1: Sum of two complex numbers is always a complex number. Therefore closer property is true.

Property 2: Clearly $(z_1 + z_2) + z_3 = z_1 + (z_2 + z_3)$ for all complex numbers z_1, z_2, z_3. Thus Associativity property is true.

Property 3: The identity element $0 = 0 + i0 \in \mathbb{C}$ and $0 + z = z + 0 = z$ for all $z \in \mathbb{C}$.

Property 4: For every $\boldsymbol{z} \in \mathbb{C}$ there exists a unique $-z \in \mathbb{C}$ such that $z + (-z) = (-z) + z = 0$.

Property 5: $z_1 + z_2 = z_2 + z_1$ for all complex numbers $\boldsymbol{z_1}$ and $\boldsymbol{z_2}$.Thus $(\mathbb{C}, +)$ is an abelian group.

Example:
Consider the set of all non-zero complex numbers $\mathbb{C}^*$under the multiplication of complex numbers.

Property 1: Product of two non-zero complex numbers is again a non-zero complex number. Therefore closer property is true.

Property 2: Clearly $(z_1 \times z_2) \times z_3 = z_1 \times (z_2 \times z_3)$ for all complex numbers z_1, z_2, z_3. Thus Associativity property is true.

Property 3: The identity element $1 = 1 + i0 \in \mathbb{C}$ and $1 \times z = z \times 1 = z$ for all $z \in \mathbb{C}$.

Property 4: Let $z = x + iy \in G$.
Here $z \neq 0 \Rightarrow x$ and $\boldsymbol{y}$ are not both zero. $\therefore x^2 + y^2 \neq 0$

$$\frac{1}{z} = \frac{1}{x + iy} = \frac{x - iy}{(x + iy)(x - iy)} = \frac{x - iy}{x^2 + y^2} = \frac{x}{x^2 + y^2} + i\left(\frac{-y}{x^2 + y^2}\right) \in G$$

Also $z \times \frac{1}{z} = \frac{1}{z} \times z = 1$.Therefore z has the inverse $\frac{\boldsymbol{1}}{\boldsymbol{z}} \in G$. Further $z_1 \times z_2 = (a + ib)(c + id) = (ac - bd) + i(ad + bc) = (ca - db) + i(da + cb) = z_2 \times z_1$.
Thus $(\mathbb{C}, \times)$ is an abelian group.
As a tabular format we summarize the axioms of a group in the order for a particular operation.

	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$	$\mathbb{Q}^* = \mathbb{Q} - \{0\}$	$\mathbb{R}^* = \mathbb{R} - \{0\}$	$\mathbb{C}^* = \mathbb{C} - \{0\}$
$+$	Semi group	Group	Group	Group	Group	Not closed	Not closed	Not closed
$\times$	Monoid	Monoid	Monoid	Monoid	Monoid	Group	Group	Group

–	Not closed	Not asso.	Not asso.	Not asso.	Not asso.	Not closed	Not closed	Not closed
÷	Not closed	Not closed	Not closed	Not closed	Not closed	Not asso.	Not asso.	Not asso.

* asso. means associative

Example:
Consider the set of all 2×2 non-singular matrices under matrix multiplication, where the entries belong to R.

Property 1: The product of two non-singular matrices is again non-singular and the order is 2×2. Therefore closer property is true.

Property 2: Clearly $(A \times B) \times C = A \times (B \times C)$ for all 2×2 matrix A, B, C. Thus Associativity property is true.

Property 3:The identity element $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ satisfies the identity property.

Property 4: Let $A \in G$.Since A is a non-singular matrices, determinant of A $det(A) \neq 0$. Therefore $A^{-1} = \frac{1}{det(A)} Adj(A) \in G$ and $A \times A^{-1} = A^{-1} \times A = I$. Thus Inverse property is true.

Property 5: Matrix multiplication is non-commutative (in general).
Hence the set of all 2×2 non-singular matrices forms a non-abelian group under matrix multiplication.

Uniqueness of Identity:
There is only one identity element in any group $\boldsymbol{G}$.

Proof:
Suppose both e and e' are identities of G.
Then
$ae = a$ for all a in G, and …….. (1)
e′a = a for all a in G…….. (2)
The choice of a = e′ in (1) and a = e in (2) yields e′ e = e′ and e′ e = e.
Thus, e and e′ are both equal to e′ e and so are equal to each other.

Cancellation Law:
The right and left cancellation laws hold for any group $\mathbf{G}$ that is,
ba = ca implies b = c, and
ab = ac implies b = c.

Proof:
Suppose ba = ca. Let a′ be an inverse of a.
Then, multiplying on the right by a′ gives $(ba)a' = (ca)a'$.
By the associativity law, we get b(aa′) = c(aa′).
Then, be = ce and, therefore, b = c as desired.

Similarly, one can prove $ab = ac$ implies $b = c$ by multiplying by a' on the left.

Uniqueness of Inverse:
For each element a in a group G, there is a unique element b in G such that $ab = ba = e$.

Proof:
Suppose b and c are both inverses of a.
Then $ab = e$ and $ac = e$. So that $ab = ac$.
By cancellation law, we get $b = c$. Therefore inverses are unique. That is, each element has exactly one inverse, and no two distinct elements have the same inverse.