Groups and Rings.

Algebraic Systems:

Binary Operation: The binary operation $*$ is said to be binary operation on set A If $a * b \in A$ for all $a, b \in A$

$*$ binary operation is an operation that combines two element to produce another element

eg① N = set of Natural numbers

$= \{1, 2, 3 \longrightarrow\}$

for $a, b \in N$ then $a + b \in N$

∴ addition is the binary operation on set of Natural numbers

But Subtraction is not binary operation

because $a = 3$ $b = 5 \in N$

But $a - b = 3 - 5 = -2 \notin N$

* Simlarly Product of two natural number is natural number But Quotient is not natural number, Therefore multiplication is binary operation But Quotient is not binary operation

(2) Σ = set of Integers

$= \{ \text{---} \quad -2 \; -1 \; 0, 1, 2 \; \text{---} \}$

addition, Subtraction and multiplication is the binary operation But Quotient is not binary operation

* Algebric System:

A system consisting of a set S and one or more binary operation defined on the set will be called as Algebric System

eg $(N, +)$, $(N, \times)$, $(Z, +, \times)$, $(Q, +, \times)$, $(R, +\times)$

* Monoid:

A non empty set A with binary operation $*$ defined on A is called Monoid

If $*$ satisfies the following properties

(i) $a * (b * c) = (a * b) * c$ for all $a, b, c \in A$

(ii) There exist an element $e \in A$ such that $a * e = e * a = a$ for any $a \in A$

e is called an identity of A

eg: $(N, \times)$ is monoid because

(i) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in N$

(ii) $\exists\ e = 1 \in N$ ($e = 1$ called multiplicative identity) such that $a \cdot e = e \cdot a = a$ for any $a \in N$

(2) $(N, +)$ is not monoid because

$e = 0 \notin N$

(additive identity 0 not present in the set of Natural numbers)

* Semigroups

Let $(A, *)$ be an Algebric System with binary operation $*$ on A

Then $(A, *)$ is said to be semigroup If $*$ is associative

ie $a * (b * c) = (a * b) * c$ for all $a, b, c \in A$

eg ① $(N, +)$ is semigroup because

for all $a, b, c \in N$

$$a + (b + c) = (a + b) + c$$

② $(N, -)$ is not semigroup because

Subtraction is not binary operation

③ $(Z, +)$, $(Z, \times)$ are semigroups

But $(Z, -)$ is not semigroup

because for $a = 2$ $b = 3$ $c = 4 \in Z$

$$2 - (3 - 4) \neq (2 - 3) - 4$$

* Semigroup: Algebric System + Associative

$(\mathbb{Z}, +)$, $(\mathbb{Z}, \times)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}, \times)$ monoid

In short

Monoid = semigroup + existence of identity

(for addition $e = 0$ and multiplication $e = 1$)

* Group:

A group is a nonempty set G with, a binary operation $*$ defined on G with the following Properties:

(I) $(a * b) * c = a * (b * c)$ for any $a, b, c \in G$

(II) There exist a unique element $e \in G$ such that $a * e = e * a$ for any $a \in G$

(III) for every $a \in G$ there is an element $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$ where a^{-1} is an inverse of a

eg ① $(Z, +)$

(i) $(a+b)+c = a+(b+c)$ for all $a, b, c \in Z$

(ii) There exist an element $e = 0 \in Z$ such that $a + e = e + a = a$ for any $a \in G$

(iii) for every $a \in Z$ there is an element $a^{-1} = (-a)$ such that

$a + (-a) = (-a) + a = e = 0$

$a^{-1} = (-a)$ is called inverse of a

$\therefore (Z, +)$ is Group under binary operation addition

② $(Z, \times)$ is not Group because for every element $a \in Z$ multiplicative inverse does not exist

($a = 2$. $\nexists\ a^{-1} \in Z$ s.t $a \cdot a^{-1} = e = 1$)

Examples of Groups

$(Q, +)$, $(R, +)$

But $(Q, \times)$ is not group because for element $a = 0$ multiplicative inverse does not exist.

Is $(Z_4, +_4)$ is Group ?

Sol'n Z_4 denotes the set of all equivalence classes generated by the equivalence relation congruent modulo 4

$$Z_4 = \{[0], [1], [2], [3]\}$$

or $Z_4 = \{0, 1, 2, 3\}$

Composition Table under binary operation addition modulo 4

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

from Composition Table

(i) Z_4 is associative under the operation "$+_4$"

(ii) There exist identity $e = 0 \in Z_4$

(iii) for every element inverse exist

element	Inverse
$a = 0$	$a^{-1} = 0$
1	3
2	2
3	1

$\therefore (Z_4, +_4)$ is Group

In general

$(Z_m, +_m)$ is Group

Ex Is $(Z_4, \times_4)$ is Group?

Composition Table

$\times_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

from Composition Table

for an element $a = 0, 2$

inverse does not exist in Z_4

$\therefore (Z_4, \times_4)$ is not Group

Is $(Z_5, \times_5)$ is Group

Sol'n $Z_5 = \{0, 1, 2, 3, 4\}$

Composition Table

$\times_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

from Composition Table

Inverse of $a=0$ does not exist in Z_5

$\therefore (Z_5, \times_5)$ is not Group

But $(Z_5^*, \times_5)$ is Group

where $Z_5^* = \{1, 2, 3, 4\}$

Abelian Group:

A group $(G, *)$ is called an abelian Group if $a * b = b * a$ for all $a, b \in G$

eg ① $(\mathbb{Z}, +)$, $(\mathbb{Z}, \times)$, $(\mathbb{Q}, +)$ $(\mathbb{R}, +)$

$(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$ abelian Groups

② $(\mathbb{Z}_m, +_m)$ is an abelian group

③ $(M_n(\mathbb{R}), \times)$ is not abelian group

($M_n(\mathbb{R})$ denotes set of $n \times n$ square matrices with real entries)

Matrix multiplication is not Commutative

Cyclic Group:

A Group $(G, *)$ is ~~Void~~ be called a Cyclic group If there exist an element $a \in G$ such that every element of G can be written as a^n for some integer n

ie $G = \{a^n \mid n \in Z\}$

we say that G is generated by a or a is generator of G

If binary operation is addition then

$$a^n = \underbrace{a + a + \cdots + a}_{n \text{ times}} = n \cdot a$$

If binary operation is multiplication then

$$a^n = \underbrace{a \times a \times \cdots \times a}_{n \text{ times}}$$

eg Show that $(Z, +)$ is Cyclic Group

Soln $Z = \{ - \text{---} -2, -1, 0, 1, 2, 3 \text{---} \}$

If $a = 0$

Then $\langle 0 \rangle = \{ n(0) \mid n \in Z \} = \{ 0 \} \neq G$

$\therefore$ 0 is not generator of Z,

If $a = 1$

$$\langle a \rangle = \{ n \cdot a \mid n \in Z \}$$

$$\langle 1 \rangle = \{ n \cdot (1) \mid n \in Z \} = Z$$

$\therefore$ 1 is generater of G

If $a = 2$

$$\langle 2 \rangle = \{ n(2) \mid n \in Z \} = 2Z \neq Z$$

$\therefore$ 2 is not generater of Z

Similarly 3, 4, 5, ——— not generater of Z

If $a = -1$

$$\langle -1 \rangle = \{n \cdot (-1) \mid n \in \mathbb{Z}\} = \mathbb{Z}$$

$\therefore -1$ is not generator of $\mathbb{Z}$

$a = -2$

$$\langle -2 \rangle = \{n \cdot (-2) \mid n \in \mathbb{Z}\} = \mathbb{Z}$$

$\therefore -2$ is not generater of $\mathbb{Z}$

Similarly $-3, -4, \ldots$ not generater of $\mathbb{Z}$

$\therefore \mathbb{Z}$ is generated by 1 and -1

$\therefore (\mathbb{Z}, +)$ is Cyclic Group

② Is $(\mathbb{Q}, +)$ is Cyclic Group

Sol: $\mathbb{Q} = \{p/q \mid q \neq 0, p, q \in \mathbb{Z}\}$

for every element $a \in \mathbb{Q}$

$$\langle a \rangle = \{n \cdot a \mid n \in \mathbb{Z}\} \neq \mathbb{Q}$$

$\therefore (\mathbb{Q}, +)$ is not Cyclic Group

* Every Cyclic group is abelian But converse need not be true

ie Cyclic Group $\Rightarrow$ Abelian

$\not\Leftarrow$

for eg $(\mathbb{Q}, +)$ is Abelian Group But not Cyclic Group

* $(\mathbb{Z}_m, +_m)$ is Cyclic Group generated by 1

Subgroup:

Let $(G, *)$ be a Group. A nonempty subset H of G is called subgroup of G If the following conditions are satisfied

(i) The identity $e \in H$

(ii) If $a, b \in H$, then $a * b \in H$

(iii) If $a \in H$ then $a^{-1} \in H$

In other words $(H, *)$ is itself a Group

For any Group $(G, *)$
$H = \{e\}$ and $H = G$ are called trivial subgroups

eg (1) for the Group $G = (\mathbb{Z}, +)$
$H = (m\mathbb{Z}, +)$ is subgroup of $(\mathbb{Z}, +)$

(2) $(\mathbb{Z}_m, +_m)$ is not subgroup of $(\mathbb{Z}, +)$ because binary operation not same

(3) $(\mathbb{Z}, +)$ is subgroup of $(\mathbb{Q}, +)$

(4) $(\mathbb{Q}, +)$ is subgroup of $(\mathbb{R}, +)$

Is $H = \{0, 2\}$ is subgroup of Z_4 under the operation addition modulo 4

Soln:

$H = \{0, 2\}$

$Z_4 = \{0, 1, 2, 3\}$

H is subset of Z_4

$+_4$	0	2
0	0	2
2	2	0

(i) $e = 0 \in H$

(ii) If $a, b \in H$ then $a +_4 b \in H$

(iii) If $a \in H$ then $a^{-1} \in H$

$\therefore H = \{0, 2\}$ is Subgroup of Z_4

Cosets:

Let $(G, *)$ be a Group and $(H, *)$ be a Subgroup of G, for any $a \in G$ the set $aH = \{a * h \mid h \in H\}$ is called the Left coset of H determined by a

Similarly $Ha = \{h * a \mid h \in H\}$ is called a Right coset of H in G determined by a

a is called as the representive element of the coset aH or Ha

eg $G = (Z_4, +_4)$ and $H = \{0, 2\}$ is Subgroup of $(Z_4, +_4)$ then

Find Left cosets and Right Cosets of H in G

Soln: $G = (Z_4, +_4)$

$H = \{0, 2\}$

$Z_4 = \{0, 1, 2, 3\}$

Left Cosets:

for $a = 0$

$$0H = \{0 + h \mid h \in H\}$$

$$0H = \{0, 2\}$$

for $a = 1$

$$1H = \{1 + h \mid h \in H\}$$

$$1H = \{1, 3\}$$

for $a = 2$

$$2H = \{2, 0\} = 0H$$

for $a = 3$

$$3H = \{3, 1\} = 1H$$

Right Cosets:

for $a = 0$

$$H0 = \{h + 0 \mid h \in H\}$$

$$H0 = \{0, 2\}$$

for $a = 1$

$H1 = \{1, 3\}$

for $a = 2$

$H2 = \{2, 1\} = H0$

for $a = 3$

$H3 = \{3, 1\} = H1$

* Normal Subgroup:

A subgroup H of G is said to be normal subgroup if for every $a \in G$, $aH = Ha$

eg $G = (Z_4, +_4)$ and $H = \{0, 2\}$ is Subgroup of $G = (Z_4, +_4)$

for every $a \in Z_4$, $aH = Ha$

$\Rightarrow$ H is Normal Subgroup of $G = (Z_4, +_4)$

* Every Subgroup of an abelain group is Normal Subgroup

eg $G = (Z, +)$ and $H = (nZ, +)$ is Normal Subgroup of $(Z, +)$