GROUPS

Let G be a non-empty set and $*$ be a binary operation defined on it, then the structure (G,$*$) is said to be a group, if the following axioms are satisfied,

(i) Closure property : $a * b \in G, \ \forall \ a, b \in G$

(ii) Associativity : The operation $*$ is associative on G. i.e.

$$a * (b * c) = (a * b) * c, \quad \forall \ a, b, c \in G$$

(iii) Existence of identity : There exists an unique element e $\in$ G, such that

$$a * e = a = e * a, \quad \forall \ a \in G$$

e is called identity of $*$ in G

(iv) Existence of inverse : for each element a$\in$ G, there exist an unique element b$\in$ G such that

$$a * b = e = b * a$$

The element b is called inverse of element a with respect to $*$ and we write $b = a^{-1}$

Abelian Group

A group (G,$*$) is said to be abelian or commutative, if

$$a * b = b * a \quad \forall\ a, b \in G$$

Some Examples of Group

The set of all 3×3 matrices with real entries of the form

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

is a group.

This group sometimes called the Heisenberg group after the Nobel prize-winning physicist Werner Heisenberg, is intimately related to the **Heisenberg uncertainity principle** of quantum physics.

Another example

The set of six transformations $f_1, f_2, f_3, f_4, f_5, f_6$ on the set of complex numbers defined by

$$f_1(z) = z,\ f_2(z) = \frac{1}{z},\ f_3(z) = 1 - z,\ f_4(z) = \frac{z}{z-1},$$

$$f_5(z) = \frac{1}{1-z},\ f_6(z) = \frac{z-1}{z}.$$

forms a finite non-abelian group of order six with respect to the composition known as the composition of the two functions or product of two functions.

Order of a Group and Order of an element of a group

Order of a Group

The number of element in a finite group is called the order of a group. It is denoted by $o(G)$.
An infinite group is a group of infinite order.

e.g.,

1. Let $G = \{1, -1\}$, then G is an abelian group of order 2 with respect to multiplication.
2. The set $\mathbb{Z}$ of integers is an infinite group with respect to the operation of addition but $\mathbb{Z}$ is not a group with respect to multiplication.

Order of an element of a group

Order of an Element of a Group

Let G be a group under multiplication. Let e be the identity element in G. Suppose, a is any element of G, then the least positive integer n, if exist, such that $a^n = e$ is said to be order of the element a, which is represented by

$$o(a) = n$$

In case, such a positive integer n does not exist, we say that the element a is of infinite or zero order.

e.g.,

(i) The multiplicative group $G = \{1, -1, i, -i\}$ of fourth roots of unity, have order of its elements

$$(1)^1 = 1 \quad \Rightarrow o(1) = 1$$

$$(-1)^2 = 1 \quad \Rightarrow \quad o(-1) = 2$$
$$(i)^4 = 1 \quad \Rightarrow \quad o(i) = 4$$
$$(-i)^4 = 1 \quad \Rightarrow \quad o(-i) = 4$$

respectively.

(ii) The additive group $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$
$1.0 = 0 \quad \Rightarrow$ order of zero is one(finite).
but $na \neq 0$ for any non zero integers a.
$\Rightarrow \quad o(a)$ is infinite.

Modular Arithmetic

Modular Arithmetic imports its concept from division algorithm ($a = qn + r, \text{where } 0 \leq \text{r} < \text{n}$) and is an abstraction of method of counting that we often use.

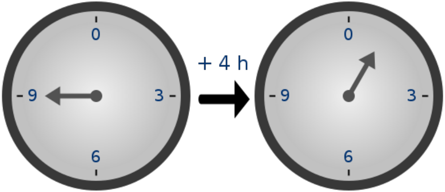
Modulo system

Let n be a fixed positive integer and a and b are two integers, we define $a \equiv b(modn)$, if $n \mid (a - b)$ and read as, "a is congruent to b mod n".

Addition modulo m and Multiplication modulo p

Let a and b are any two integers and m and p are fixed positive integers, then these are defined by
$a +_m b = r, \quad 0 \leq r < m$, and
$a \times_p b = r \quad 0 \leq r < p$ where r is the least non-negative remainder ,whern $a + b$ and $a.b$ divided by m and p respectively.

Examples. (i) The set $\{0, 1, 2, 3, ...(n-1)\}$ of n elements is a finite abelian group under addition modulo n.



Time-keeping on this clock uses arithmetic modulo 12.

(ii) **Fermat's Little theorem :** If p is prime, then $a^{p-1} \equiv 1(modp)$ for $0 < a < p$.

(iii) **Euler's theorem** if a and n are co-prime, then

$$a^{\phi(n)} \equiv 1(modn),$$

where ϕ is Euler's totient function.

Subgroup

Definition

A non-empty subset H of a group $(G, *)$ is said to be subgroup of G, if $(H, *)$ is itself a group.

e.g., [{1,-1}, .] is a subgroup of [{1,-1,i,-i} .]

Criteria for a Subset to be a Subgroup

A non-empty subset H of a group G is a subgroup of G if and only if

(i) $a, b \in H \Rightarrow ab \in H$

(ii) $a \in H \Rightarrow a^{-1} \in H$,

where a^{-1} is the inverse of $a \in G$

Lagrange's Theorem

Statement

The order of each subgroup of a finite group is a divisor of the order of the group.

i.e., Let H be a subgroup of a finite group G and let

$$o(G) = n \quad \text{and} \quad o(H) = m, \text{ then}$$

$$m \mid n \qquad \text{(m divides n)}$$

Since, $f : H \to aH$ and $f : H \to Ha$ is one-one and onto.
$\Rightarrow o(H) = o(H) = m$

Now, $\quad G = H \cup Ha \cup Hb \cup Hc \cup \ldots$, where a,b,c,...$\in G$

$$\Rightarrow \quad o(G) = o(H) + o(Ha) + o(Hb) + \ldots$$

$$\Rightarrow \quad n = m + m + m + m + \ldots. + \text{ upto } p \text{ terms} \qquad \text{(say)}$$

$\Rightarrow \quad n = mp$

$\Rightarrow$ Order of the subgroup of a finite group is a divisor of the order of the group.

※ ※ ※

$\star$ The converse of Lagrange's theorem is not true.

e.g.,

Consider the symmetric group P_4 of permutation of degree 4. Then $o(P_4) = 4! = 24$ Let A_4 be the alternative group of even permutation of degree 4. Then, $o(A_4) = \dfrac{24}{2} = 12.$ There exist no subgroup H of A_4, such that $o(H) = 6$, though 6 is the divisor of 12.