LECTURE-4

Now, that we know what a group is, we would like to increase our understanding of it. One of the important ways to understand a group is through its subgroups. This is what we are going to study now.

As the name suggests, subgroups are subsets of a group, which themselves are groups. To understand this let's see an example:-

Example 1- Consider the group $(\mathbb{Z}, +)$

1.1) let $2\mathbb{Z} = \{\ldots -6, -4, -2, 0, 2, 4 \ldots\} \subset \mathbb{Z}$

one can easily check that $2\mathbb{Z}$ satisfies all the properties of a group under addition & $\because$ $2\mathbb{Z} \subset \mathbb{Z} \Rightarrow (2\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$.

1.2) Now, consider the set $\{-1, 0, 1\} \subset \mathbb{Z}$.

$\{-1, 0, 1\}$ contains the additive identity (i.e. 0) and also the inverse of every element but it is not a group $\because 1+1 = 2 \notin \{-1, 0, 1\}$. Hence it is not a subgroup of $(\mathbb{Z}, +)$.

So finally let's see the definition of a subgroup.

<u>Definition</u>:- Let $(G, \cdot)$ be a group. A subset H of G is called a SUBGROUP of G if it itself is a group under the operation "$\cdot$". and we write $H \leq G$

<u>Remark</u>:- It is important to note that H must be a group under the same operation as that of G.

<u>Exercise</u>:- Try to find some subgroups of all the examples of groups that we have seen.

Observe that every group comes equipped with two subgroups; <u>the identity</u> & the <u>whole group</u>. ($\{e\}$ is called the "trivial subgroup".)

A subgroup H of G is called a "proper subgroup". if it not the trivial subgroup or the group G itself.

Subgroup Generated by an element:-

Before discussing subgroups generated by an element, let's see some definitions:

<u>Definition</u>:- Let $a, b \in G$, for any $k \in \mathbb{Z}$, the element $a^k \in G$ is defined by

$$a^k = \begin{cases} \underbrace{a.a.a \ldots a}_{k\text{-times}} & , k > 0 \\ e & , k = 0 \\ \underbrace{a^{-1}.a^{-1} \ldots a^{-1}}_{k\text{-times}} & , k < 0 \end{cases}$$

<u>Exercise</u>:- Prove that $\forall n, m \in \mathbb{Z}$, $a^n . a^m = a^{n+m}$ and $(a^n)^{-1} = a^{-n}$ (ie the laws of exponents hold for elements in a group)

<u>Definition</u>:- (Order of an element)

Let $a \in G$, the order of a, denoted by ord(a) is the smallest positive integer k such that $a^k = e$. If there is no such $k \in \mathbb{Z}$, ord$(a) = \infty$.

<u>Example</u> 1- Consider $(\mathbb{Z}_6, +)$, and consider the element $3 \in \mathbb{Z}_6$. From previous definition

$3^k = \underbrace{3 + 3 + \ldots 3}_{k\text{-times}} \pmod 6$, so the ord$(a) = 2$ as

$3+3 = 6 \equiv 0 \pmod 6$, which is the identity in $\mathbb{Z}_6$.

2- Consider $(\mathbb{Z},+)$, and consider $2 \in \mathbb{Z}$. Clearly $\nexists\ k \in \mathbb{Z}$ st $2^k = \underbrace{2+2+\dots 2}_{k \text{ times}} = 0$
$\Rightarrow$ $\operatorname{ord}(2) = \infty$.

<u>Definition</u>:- Let $a \in G$, the "subgroup generated by a" denoted by $\langle a \rangle$, is defined as

$$\boxed{\langle a \rangle = \{ a^k \mid k \in \mathbb{Z} \}}$$

for example for $2 \in \mathbb{Z}$, $\langle 2 \rangle$ is just the set of even integers which we already proved to be a subgroup of $\mathbb{Z}$.

Even though it seems that $\langle a \rangle$ is always an infinite set, it can be finite.

for example, consider $3 \in \mathbb{Z}_6$ again then,

$$\langle 3 \rangle = \{ 0, 3 \}.$$

Note that, $|\langle 3 \rangle| = \text{ord}(3)$, this is not a coincidence !!, in fact

<u>Exercise</u> - show that $|\langle a \rangle| = \text{ord}(a)$, for $a \in G$

<u>Remark</u> - Not all subgroups of a group are generated by a single element of the group.
for example, consider $\mathbb{Z}_4 \times \mathbb{Z}_4$ and consider the subgroup $H = \{(0,0), (0,2), (2,0), (2,2)\}$, then this is not a subgroup generated by a single element.

———— × ———— × ———— × ————