Lecture 3

We'll start by defining the order of an element

Definition Let $(G, \cdot)$ be a group and $k \in \mathbb{Z}$. The element $a^k \in G$ is defined by

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

Exercise [Laws of exponents hold in a group].
Let G be a group, $a \in G$ and $n, m \in \mathbb{Z}$. Prove that $a^n \cdot a^m = a^{n+m}$ and $(a^n)^{-1} = a^{-n} = (a^{-1})^n$.

We now make the following definition

Def:- [Order of an element]

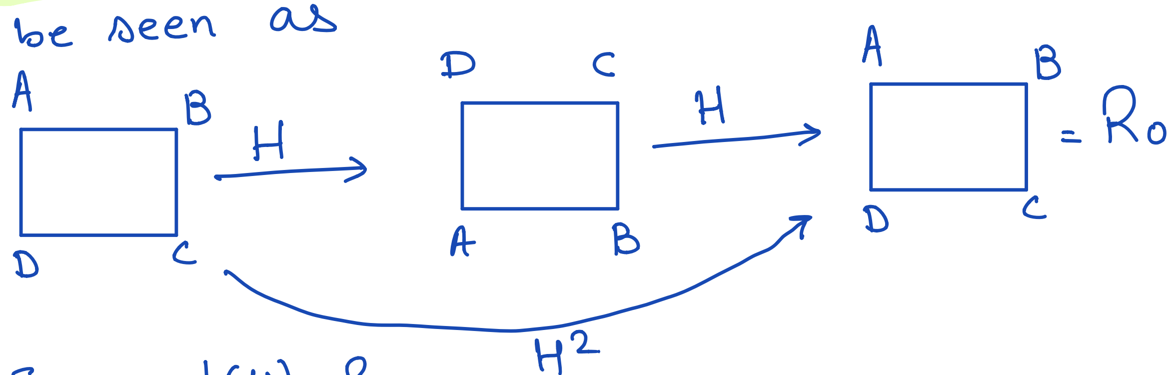
Let G be a group and $a \in G$. The order of a, denoted by $\text{ord}(a)$ is the smallest positive integer k such that $a^k = e$. If there is no such $k \in \mathbb{Z}$, then we say $\text{ord}(a) = \infty$.

e.g. ① Consider $U(12) = \{1, 5, 7, 11\}$. Then

$5^2 = 25 \equiv 1 \bmod (12)$ and 2 is the smallest positive integer with this property. So

$\text{ord}(5) = 2$.

② Consider D_4 and $H \in D_4$. Then H^2 can be seen as



So, $\text{ord}(H) = 2$.

③ In $(\mathbb{Z}, +)$, any non-zero element has order ∞.

Examples continued

Permutation or Symmetric groups

Let's look at another important set of examples called the permutation or the symmetric groups, denoted by S_n, $\forall n \geq 1$. Even though, we can define S_n for every $n \geq 1$, here we'll only focus on S_3 (the first interesting case) and will come back to their study in depth later.

first a definition

__Definition__ Let B be a non-empty set. A permutation of B is a function from B to B which is a bijection, i.e., it is both one to one and onto.

Even though, the notion of permutation makes sense for an infinite set B, here we'll focus on the case when B is finite so for convenience, we can take $B = \{1, 2, \ldots, n\}$ if it has n elements.

So if $B = \{1, 2, 3, 4\}$, for instance, then one possible permutation of B could be the function $\alpha : B \longrightarrow B$ given by $\alpha(1) = 2$, $\alpha(2) = 3$, $\alpha(3) = 4$ and $\alpha(4) = 1$ or a function β given by

$\beta(1) = 3$, $\beta(2) = 2$, $\beta(3) = 4$ and $\beta(4) = 1$.

So you can see that there can be many permutations on a set.

The group S_3

Now let $B = \{1, 2, 3\}$ and let S_3 denote the set of all permutations on B. Then S_3 is a group called the symmetric or permutation group on 3 letters.

So there are two questions :-

1) What is the group operation?
2) How many elements does S_3 have and what are they?

To answer the first question, Observe that S_3 is the set of functions from $B \to B$. and if we want S_3 to be a group, so the operation must take two functions and return a single function. So there is an obvious operation on functions : composition of two functions. and this is the group operation on S_3.

So one can ask, how does this operation works on S_3? For that we'll have answer the second question.

First let's see how many elements can S_3 have? $\to$

If we have any bijection on $\{1,2,3\}$ then we know that the element 1 has a total of three choices to be mapped to ; 1, 2 or 3. Once 1 is mapped to an element, 2 has now two choices only as the function must be one-to-one. Once 2 has been mapped then 3 now has only one choi--ce.

So total we have $3 \cdot 2 \cdot 1 = 3! = 6$ choices for a function on $\{1,2,3\}$ to be bijection and so S_3 has 6 elements.

Remark :- In fact, S_n has $n!$ elements.

Now the question is that what are the elements of S_3?

One obvious element is the function $\epsilon : \{1,2,3\} \longrightarrow \{1,2,3\}$ given by $\epsilon(1) = 1$, $\epsilon(2) = 2$ and $\epsilon(3) = 3$.

Another way to write this function is

$$\epsilon = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}$$

where the top row should be conside-
-red as elements of B in the domain and the bottom row is the co-domain.

So the above array is telling us that

$1 \longrightarrow 1$, $2 \longrightarrow 2$ and $3 \longrightarrow 3$

Let's consider another element of S_3

$\alpha : B \longrightarrow B$, $\alpha(1) = 2$, $\alpha(2) = 3$ and $\alpha(3) = 1$

which in the array form can be written as

$$\alpha = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$$

Now if $\alpha \in S_3$ and S_3 is a group then $\alpha \cdot \alpha$ must be in S_3.

Since the group operation is the composition of functions $\Rightarrow$

$$\alpha^2 = \alpha \cdot \alpha = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$$

What about α^3? $\alpha^3 = \alpha^2 \cdot \alpha = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}$ which is the same as ϵ and so it's not a new element.

Another element of S_3 is

$$\beta = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$$

Again $\alpha \cdot \beta \in S_3$ because S_3 is a group.

and for finding $\alpha \circ \beta$ we recall that in the composition of two functions, we move from right to left, i.e, first apply β then α. So

$$\alpha \circ \beta = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$$

which is a new element.

finally $\beta \circ \alpha = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$ which is again a new element and so we got all the elements of the group and so

$$S_3 = \{ \epsilon, \alpha, \beta, \alpha^2, \alpha\beta, \beta \circ \alpha \}$$

Observe that $\alpha \cdot \beta \neq \beta \circ \alpha$ so S_3 is

non-abelian.

<u>Remark</u> One can ask that after finding β, we did $\alpha \cdot \beta$. Why didn't we do $\alpha^2 \cdot \beta$?

Exercise Check that $\alpha^2 \cdot \beta = \beta \cdot \alpha$.

Before moving on, let's make a definition :-

Definition (order of a group)

Let $(G, \cdot)$ be a group. The order of the group G, denoted by $|G|$, is the number of elements in the group.

e.g. order of $(\mathbb{Z}, +)$ is infinite.

$$|D_4| = 8$$

$$|S_3| = 6$$

New groups from old - Direct product of groups

Given two groups G and H, we can form a new group called the direct product (or external direct product).

Definition Let $(G, \circ)$ and $(H, *)$ be groups. The direct product of G and H is defined as the group $(G \times H, \cdot)$ where

$$G \times H = \{ (g, h) \mid g \in G,\ h \in H \}$$

and $(g_1, h_1) \cdot (g_2, h_2) = (g_1 \circ g_2,\ h_1 * h_2)$ $\forall\ g_1, g_2 \in G$ and $h_1, h_2 \in H$.

Exercise Prove that $(G \times H, \cdot)$ is a group.