Discrete Structures and Theory of Logic

Lecture-14

Dharmendra Kumar

July 23, 2020

Order of a group

The order of a group(G,o) is the number of elements of G, when G is finite. If G is infinite, then the order will be infinite.

Example: Consider the multiplicative group G = { 1, -1, i, , -i}. Since this group is finite, therefore the order of this group is 4.

Example: Show that the set $\{1,2,3,4,5\}$ is not a group under addition and multiplication modulo 6 operation.

Solution: The composition tables under addition and multiplication modulo 6 operations are the following:-

$+_6$	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4

$\times_6$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

Closure property is not satisfied under both operation, because 0 entry belongs into table which is not the element of set. Therefore, the set $\{1,2,3,4,5\}$ is not a group under addition and multiplication modulo 6 operation.

Example: Prove that the set {0,1,2,3,4} is a finite abelian group of order 5 under addition modulo 5 operation.

Solution: The composition tables under addition and multiplication modulo 6 operations are the following:-

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

From table, closure property is satisfied, because all entries of table belongs into set {0,1,2,3,4}.

Group

Since operation is addition, therefore associative property is satisfied. Clearly from table, identity element is 0. And each element has a inverse i.e. $(0)^{-1} = 0$, $(1)^{-1} = 4$, $(2)^{-1} = 3$, $(3)^{-1} = 2$, $(4)^{-1} = 1$. Commutative property is also satisfied because aob = boa, for all a,b.
Therefore, this set is an abelian group under operation $+_5$.

Left cancellation law
For a,b,c $\in$ G, aob = aoc $\Leftrightarrow$ b = c.
Right cancellation law
For a,b,c $\in$ G, boa = coa $\Leftrightarrow$ b = c.

Example: In a group (G,o), prove the following:-

(a) $(a^{-1})^{-1} = \text{a}$

(b) $(aob)^{-1} = b^{-1}oa^{-1}$

Solution:

(a) Since a^{-1} is the inverse of a, therefore aoa^{-1} = e ....(1)

Since a $\in$ G, therefore a^{-1} is also belong into G. Since $a^{-1} \in$ G, therefore inverse of it will also belong.

Using inverse property, $(a^{-1})^{-1}oa^{-1} = \text{e}$ ....(2)

Using (1) and (2), $(a^{-1})^{-1}oa^{-1} = aoa^{-1}$

By right cancellation law, we get $(a^{-1})^{-1} = \text{a}$

It is proved.

Group

(b) Consider a,b $\in$ G. Therefore, its inverses are a^{-1} and b^{-1}.
Since a,b $\in$ G, therefore aob also belong into G.
Now, $b^{-1}oa^{-1}$ will be inverse of aob if (aob)o $(b^{-1}oa^{-1}) =$ e.
Now, (aob)o $(b^{-1}oa^{-1}) =$ ao(bo$(b^{-1}oa^{-1})$) using associative property

$= $ ao((bob^{-1})oa^{-1})) using associative property

$= $ ao(eoa^{-1}) since b^{-1} is the inverse of b

$= $ aoa^{-1} using identity property

$= $ e since a^{-1} is the inverse of a

Therefore, $(aob)^{-1} = b^{-1}oa^{-1}$

Example: Prove that in a group (G,o), if a^2 = a, then a = e, for a $\in$ G and e is the identity element of G.

Solution:

Since $a^2 = a \Rightarrow aoa = aoe$

$\Rightarrow a = e$ using left cancellation law.

Example: Show that if every element of a group (G,o) be its own inverse, then it is an abelian group. Is the converse true?

Solution:

First part:

Consider two elements a,b $\in$ G. Since each element has its own inverse, therefore $a^{-1} = a$ and $b^{-1} = b$.

To show that the group (G,o) is abelian, we have to show that aob = boa.

Since a,b $\in$ G, therefore aob also belong into G. Since each element has its own inverse, therefore $(aob)^{-1} = aob$

We know that $(aob)^{-1} = b^{-1}oa^{-1}$, therefore $b^{-1}oa^{-1}$ = aob $\Rightarrow$ boa = aob (Since $a^{-1} = a$ and $b^{-1} = b$)

Therefore the group is abelian.

Second part:

In this part, we have to check if a group is abelian then each element has its own inverse.

This part is not true. We are giving justification of it below.

Consider an abelian group (Z,$+$). Clearly in this group, inverse of any element a will be -a, which is not equal to a. Therefore, converse part not true.

Exercise

1. If (G,o) is an abelian group, then for all a,b $\in$ G, show that $(aob)^n = a^n \text{o} b^n$.
2. Write down the composition tables for $(Z_7, +_7)$ and $(Z_7^*, \times_7)$, where $Z_7^* = Z_7 - \{0\}$.

Order of an element

The order of an element **a** in a group (G,o) is the smallest positive integer n such that a^n = e, where e is the identity element of G. If no such integer exists, then we say a has infinite order.

Example: Let G = {1,-1,i,-i} be a multiplicative group. Find the order of every element.

Solution: In this group, the identity element, e = 1. Therefore,
$(1)^1 = 1$ (That is e.), therefore order of 1 = 1.
$(-1)^1 =$ -1, $(-1)^2 = 1$, therefore order of -1 = 2.
$(i)^1 =$ i, $(i)^2 =$ -1, $(i)^3 =$ -i, $(i)^4 = 1$, therefore order of i = 4.
$(-i)^1 =$ -i, $(-i)^2 =$ -1, $(-i)^3 =$ i, $(-i)^4 = 1$, therefore order of -i = 4.

Example: Find the order of every element in the multiplicative group G=$\{a, a^2, a^3, a^4, a^5, a^6 = e\}$.

Solution: In this group, the identity element, e = a^6. Therefore,
$(a)^6$ = e, therefore order of a = 6.
$(a^2)^1 = a^2$, $(a^2)^2 = a^4$, $(a^2)^3 = a^6$ = e, therefore order of $a^2 = 3$.
$(a^3)^1 = a^3$, $(a^3)^2 = a^6$ = e, therefore order of $a^3 = 2$.
$(a^4)^1 = a^4$, $(a^4)^2 = a^8 = a^6 o a^2 = eoa^2 = a^2$,
$(a^4)^3 = a^12 = a^6 o a^6$ = eoe = e, therefore order of $a^4 = 3$.
$(a^5)^1 = a^5$, $(a^5)^2 = a^10 = a^6 o a^4 = eoa^4 = a^4$,
$(a^5)^3 = a^15 = a^6 o a^6 o a^3 = eoeoa^3 = a^3$
$(a^5)^4 = a^20 = a^6 o a^6 o a^6 o a^2 = eoeoeoa^2 = a^2$
$(a^5)^5 = a^25 = a^6 o a^6 o a^6 o a^6 o a = eoeoeoeoa$ = a
$(a^5)^6 = a^30 = a^6 o a^6 o a^6 o a^6 o a^6 = eoeoeoeoe$ = e
Therefore, the order of $a^5 = 6$.
$(a^6)^1 = a^6$ = e, therefore order of $a^6 = 1$.