Discrete Structures and Theory of Logic

Lecture-15

Dharmendra Kumar

July 23, 2020

Cyclic group

A group (G,o) is said to be a cyclic group if there exists an element a∈G such that every element of G can be written as some power of a, that is a^n for some integer n. a is said to be the generator of G.

Example: Show that the set of integers with respect to $+$ operation is cyclic group.

Solution: A group will be cyclic if there exists a generator in the group.

Consider an element 1 of this group.

$(1)^1 = 1$

$(1)^2 = 1+1 = 2$

$(1)^3 = 1+1+1 = 3$

$(1)^4 = 1+1+1+1 = 4$

Clearly 1, 2, 3, 4 are expressed in the power of 1. Similarly, we can expressed all the positive integers in the power of 1.

Cyclic group

Now, $(1)^{-1} = \text{-}1$
$(1)^{-2} = (1^{-1})^2 = (-1)^2 = \text{-}1\text{+}(\text{-}1) = \text{-}2$
$(1)^{-3} = (1^{-1})^3 = (-1)^3 = \text{-}1\text{+}(\text{-}1)\text{+}(\text{-}1) = \text{-}3$
$(1)^{-4} = (1^{-1})^4 = (-1)^4 = \text{-}1\text{+}(\text{-}1)\text{+}(\text{-}1)\text{+}(\text{-}1) = \text{-}4$
Clearly -1, -2, -3, -4 are expressed in the power of 1. Similarly, we can expressed all the negative integers in the power of 1.
Now, $(1)^0 = 0$
Clearly, all the integers are expressed in the powers of 1. Therefore, 1 is the generator of this group. Since generator exists, therefore the group is cyclic.

Cyclic group

Example: Is $(G, +_6)$ a cyclic group, where $G = \{0,1,2,3,4,5\}$.

Solution: We have to find generator in this group.

Consider an element 1 of this group.

Now, $(1)^1 = 1$

$(1)^2 = 1 +_6 1 = 2$

$(1)^3 = 1 +_6 1 +_6 1 = 3$

$(1)^4 = 1 +_6 1 +_6 1 +_6 1 = 4$

$(1)^5 = 1 +_6 1 +_6 1 +_6 1 +_6 1 = 5$

$(1)^6 = 1 +_6 1 +_6 1 +_6 1 +_6 1 +_6 1 = 0$

Clearly all the elements of G are expressed in the power of 1, therefore 1 is a generator of G. Since generator exists, therefore the group is cyclic.

Example: Is the multiplicative group $\{1, \omega, \omega^2\}$, a cyclic group?
Solution: Consider an element ω of G.
Now, $(\omega)^1 = \omega$
$(\omega)^2 = \omega^2$
$(\omega)^3 = \omega^3 = 1$
Clearly all the elements of G are expressed in the power of ω, therefore ω is a generator of G. Since generator exists, therefore the group is cyclic.

Cyclic group

Example: Show that every cyclic group is an abelian group.

Solution: Consider (G,o) is a cyclic group. Since (G,o) is cyclic, therefore generator exists. Let it's generator is a.

Consider two elements b,c $\in$ G. It can be expressed in the power of a. Let b $= a^i$ and c $= a^j$.

Now, boc $= a^i o a^j$

$= a^{i+j}$

$= a^{j+i}$ (since set of integers with respect to addition operation is an abelian)

$= a^j o a^i$

$=$ cob

That is, boc $=$ cob

Therefore group (G,o) is an abelian. Now, we can say, every cyclic group is an abelian group.

Cyclic group

Example: Show that if a is a generator of a cyclic group G, then a^{-1} is also a generator of G.

Solution: Since a is a generator of G, therefore each elements of G can be epressed in the power of a.

Consider any element b $\in$ G such that b $= a^i$. If we can epressed b in the power of a^{-1}, then a^{-1} will be also generator of G.

Now, b $= a^i = (a^{-1})^{-i}$. Clearly b is expressed in the power of a^{-1}, therefore a^{-1} is also generator of G.

Cyclic group

Example: How many generators are there of the cyclic group G of order 8?

Solution: Since the group is cyclic, therefore there exists generator in this group. Let a is a generator.

Therefore, G=$\{a, a^2, a^3, a^4, a^5, a^6, a^7, a^8 = e\}$.

Now, consider an element a^2.

$(a^2)^1 = a^2$

$(a^2)^2 = a^4$

$(a^2)^3 = a^6$

$(a^2)^4 = a^8 =$ e

$(a^2)^5 = a^10 = a^2$

Clearly elements a^1, a^3, a^5, a^7 are not expressed in the power of a^2.

Therefore a^2 is not generator.

Cyclic group

Now, consider an element a^3.

$(a^3)^1 = a^3$

$(a^3)^2 = a^6$

$(a^3)^3 = a^9 = \mathrm{a}$

$(a^3)^4 = a^12 = a^4$

$(a^3)^5 = a^15 = a^7$

$(a^3)^6 = a^18 = a^2$

$(a^3)^7 = a^21 = a^5$

$(a^3)^8 = a^24 = a^8 = \mathrm{e}$

Clearly all the elements of G are expressed in the power of a^3, therefore a^3 is a generator of G.

Cyclic group

Now, consider an element a^4.

$(a^4)^1 = a^4$

$(a^4)^2 = a^8 = \mathrm{e}$

$(a^4)^3 = a^{1}2 = a^4$

Clearly elements a^1,a^2, a^3, a^5,a^6, a^7 are not expressed in the power of a^4. Therefore a^4 is not a generator.

Now, consider an element a^5.

$(a^5)^1 = a^5$

$(a^5)^2 = a^{1}0 = a^2$

$(a^5)^3 = a^{1}5 = a^7$

$(a^5)^4 = a^{2}0 = a^4$

$(a^5)^5 = a^{2}5 = a$

$(a^5)^6 = a^{3}0 = a^6$

$(a^5)^7 = a^{3}5 = a^3$

$(a^5)^8 = a^{4}0 = a^8 = \mathrm{e}$

Cyclic group

Clearly all the elements of G are expressed in the power of a^5, therefore a^5 is a generator of G.
Similarly, we can show that a^7 is a generator and a^6 is not generator.
Therefore the generators of this group are a, a^3, a^5, a^7. Total number of generators is 4.

Example: Show that the group $(\{ 1,2,3,4,5,6\}, \times_7)$ is cyclic. How many generators of this group?

Solution:

Consider the element 3 of this group.

$(3)^1 = 3$

$(3)^2 = 3 \times_7 3 = 2$

$(3)^3 = 3 \times_7 3 \times_7 3 = 6$

Cyclic group

$(3)^4 = 3 \times_7 3 \times_7 3 \times_7 3 = 4$

$(3)^5 = 3 \times_7 3 \times_7 3 \times_7 3 \times_7 3 = 5$

$(3)^6 = 3 \times_7 3 \times_7 3 \times_7 3 \times_7 3 \times_7 3 = 1$

Clearly all the elements of G are expressed in the power of 3, therefore 3 is a generator of G.

Since generator exists, therefore the group is cyclic.

Another generator will be 5. Because,

$(5)^1 = 5$

$(5)^2 = 5 \times_7 5 = 4$

$(5)^3 = 5 \times_7 5 \times_7 5 = 6$

$(5)^4 = 5 \times_7 5 \times_7 5 \times_7 5 = 2$

$(5)^5 = 5 \times_7 5 \times_7 5 \times_7 5 \times_7 5 = 3$

$(5)^6 = 5 \times_7 5 \times_7 5 \times_7 5 \times_7 5 \times_7 5 = 1$

No other elements will be generator. Therefore number of generators is 2 i.e. 3 and 5.