Discrete Structures and Theory of Logic

Lecture-16

Dharmendra Kumar

July 23, 2020

Subgroup

Let (G,o) be a group and H is a subset of G. (H,o) is said to be a subgroup of (G,o) if (H,o) is also a group by itself.

Note: (G,o) and ({e},o) are the improper subgroups or trivial subgroups of (G,o).

Subgroup

Example: Is the subset {1,-1} a subgroup of multiplicative group {1, -1, i, -i}?

Solution: We have to check all the properties of group is satisfied with in set {1,-1} under multiplication operation.

Now, 1*1 = 1, 1*-1 = -1, and -1*(-1) = 1. Clearly the results of these operation are 1 and -1. And both elements belong in to given subset {1,-1}. Therefore closure property is satisfied. Since {1,-1} is subset of set {1,-1,i,-i}, therefore associative property is satisfied with in {1,-1}. Clearly 1 is identity element and it is belong into {1,-1} , therefore existence of identity property is also satisfied.

Now, 1*1 = 1, and -1*(-1) = 1. Therefore, inverse of 1 is 1 and inverse of -1 is -1. Since each element has its inverse, therefore subset {1,-1} is satisfied inverse property.

Clearly, this subset satisfies all the property, therefore this is group. And it will also be subgroup of {1,-1,i,-i}.

Subgroup

Example: Is the set of even integers a subgroup of additive group of integers?

Solution: Let I be the set of integers and H be the set of even integers.

If we add any two even integers, then we get also an integer. Therefore, addition operation satisfies closure property with in H.

Since H is a subset of I, therefore associative property is also satisfied in H.

Clearly 0 is an identity element and it also belong into H, therefore, identity property is also satisfied in H.

Consider an element $a \in H$. Clearly, $a+(-a) = 0$, therefore -a is the inverse of a. And -a is also belong into H. Therefore, inverse property is satisfied in H.

Clearly, this subset satisfies all the property, therefore this subset H is group. And it will also be subgroup of I.

Subgroup

Theorem: The identity of a subgroup is the same as that of the group.

Proof: Let H be the subgroup of G and e and e' are the identity elements of G and H respectively.

Let $a \in H$. Then

$aoe' = a$ ....(1)

Since $a \in H \Rightarrow a \in G$, therefore

$aoe = a$ ....(2)

from (1) and (2), $aoe' = aoe$

$\Rightarrow e' = e$ (using left cancellation law)

Therefore, the identity of a subgroup is the same as that of the group.

Subgroup

Theorem: The inverse of an element of a subgroup is the same as the inverse of the same regarded as an element of the group.

Proof: Let H be a subgroup of G..

Let a $\in$ H. Let b and c are the inverses of element a in H and g respectively. Therefore,

aob = e' ....(1)

and aoc = e ....(2)

From previous theorem, e' = e

Therefore, aob = aoc

$\Rightarrow$ b = c (using left cancellation law)

Therefore, the inverse of an element of a subgroup is the same as the inverse of the same regarded as an element of the group.

Subgroup

Theorem: A non-empty subset H of a group G is a subgroup of G iff

(a) a $\in$ H, b $\in$ H $\Rightarrow$ aob $\in$ H.

(b) a $\in$ H $\Rightarrow$ $a^{-1} \in$ H, where a^{-1} is the inverse of a in G.

Proof:

Necessary part:

Suppose H is a subgroup of G.

Since H is a subgroup of G, therefore closure property is satisfied within H.

So, a $\in$ H, b $\in$ H $\Rightarrow$ aob $\in$ H. Clearly part (a) is proved.

Let a $\in$ H. Since H $\subseteq$ G, therefore a $\in$ G. Let a^{-1} is the inverse of a in G. Since the inverse of an element in subgroup and group is same, therefore $a^{-1} \in$ H. Clearly, part (b) is also proved.

Subgroup

Sufficient part:

Suppose given two statements (a) and (b) are true.

Using statement (a), closure property is satisfied within H.

Since H is a subset of G and G is a group, therefore associative property is also satisfied within H.

Using statement (b), if a $\in$ H then a^{-1} $\in$ H. therefore inverse property is also satisfied within H.

Now, consider a $\in$ H $\Rightarrow$ a $\in$ H and a^{-1} $\in$ H (since inesr property is satisfied)

$\Rightarrow$ aoa^{-1} $\in$ H (using statement (a))

$\Rightarrow$ e $\in$ H, where e is an identity element.

Therefore, identity property is also satisfied within H. Clearly, all the four properties of group is satisfied within H. Therefore, H is a subgroup of G.

Theorem: The necessary and sufficient condition for a non-empty subset H of a group (G,o) to be a subgroup is

$$a \in H,\ b \in H \Rightarrow a o b^{-1} \in H$$

Where b^{-1} is the inverse of b in G.

Proof:

Necessary part:

Suppose H is a subgroup of G.

Let a$\in$ H and b $\in$ H. Since H is subgroup, therefore $b^{-1} \in$ H using inverse property.

Now, a$\in$ H and $b^{-1} \in$ H. By using closure property, ao$b^{-1} \in H$. Therefore the given statement is proved.

Sufficient part:

Suppose a$\in$H, b$\in$H $\Rightarrow$ ao$b^{-1} \in H$ ....(1)

Now, we have to show that H is a subgroup of G.

Identity property:

a$\in$H , a$\in$H $\Rightarrow$ ao$a^{-1} \in H$ (using statement (1))

$\Rightarrow$ e $\in H$

Here, e is the identity element. Therefore, identity property is satisfied within H.

Inverse property:

Now, e $\in H$, a$\in$H $\Rightarrow$ eo$a^{-1} \in H$ (using statement (1))

$\Rightarrow a^{-1} \in H$

Therefore, inverse property is satisfied within H.

Subgroup

Associative property:

Since H $\subseteq$ G, therefore associative property is also satisfied within H, because G is a group.

Closure property:

consider a$\in$H, b$\in$H $\Rightarrow$ a$\in$H, b^{-1} $\in$H

$\Rightarrow$ ao$(b^{-1})^{-1} \in H$ (using statement (1))

$\Rightarrow$ aob $\in$ H

Therefore, closure property is satisfied within H.

Clearly all the four properties are satisfied within H, therefore H is a subgroup of G.

It is proved.

Subgroup

Example: Let G $= \{$ ....,$3^{-2}, 3^{-1}, 1, 3, 3^2, 3^3$,..............$\}$ be the multiplicative group. Let H $= \{$1,3,$3^2, 3^3$,................$\}$. Is H a subgroup of G.

Solution: Clearly H is a subset of G, therefore it may be subgroup. If a$\in$H, b$\in$H $\Rightarrow$ ao$b^{-1} \in H$ is satisfied for each elements a,b $\in$ H, then H will be subgroup.

Consider a $=$ 3 and b$=$ 3^3.

Now, ao$b^{-1} = 3\text{o}(3^3)^{-1}$

$= 3\text{o}3^{-3}$

$= 3^{-2}$

Clearly this element i.e. $3^{-2} \notin$ H, therefore H is not subgroup of G.