4.3 Subgroups

Define Subgroups

Let (G, $*$) be a group. Then (H, $*$) is said to be subgroup of (G, $*$) if $H \subseteq G$ and (H, $*$) itself is a group under the operation $*$

i.e., (H, $*$) is said to be a subgroup of (G, $*$) if

- $e \,\varepsilon\, H$, where e is the identity in G.
- For any $a \,\varepsilon\, H$, $a^{-1} \,\varepsilon\, H$
- For a, $b \,\varepsilon\, H$, $a * b \,\varepsilon\, H$

Define Trivial and Proper Subgroups

- $(\{e\}, *)$ and $(G, *)$ are trivial subgroups of $(G, *)$.
- All other subgroups of $(\boldsymbol{G}, *)$ are called proper subgroups.

Examples of Subgroups:

- (Z, +) is a Subgroup of (Q, +)
- (Q, +) is a Subgroup of (R, +)
- (R, +) is a Subgroup of(C,+)

Example of Subgroups

Find all the subgroups (z_{12},$+_{12}$)

Solution:

z_{12} = {0, 1, 2, 3, 4, 5, 6, 7,8,9, 10, 11}

- Let S_1 = {0, 6}
- S_2 = {0, 4,8}
- S_3 = {0, 3, 6, 9}
- S_4 = {0, 2, 4, 6, 8}
- S_1, S_2, S_3, S_4 are proper subgroups of (z_{12}, $+_{12}$)
- ({0}, $+_{12}$) and (z_{12}, $+_{12}$) are its trivial subgroup

Theorems on Subgroups:

Theorem: 1

State and prove the necessary and sufficient condition for a subset of a group to be subgroup.

Statement:

Let (G, $*$) be a group. H is a nonempty subset of G, then H is a subgroup of G

if and only if whenever $\boldsymbol{a}, \boldsymbol{b} \in \boldsymbol{H} \Rightarrow \boldsymbol{a} * \boldsymbol{b}^{-1} \in \boldsymbol{H}$ for all

$\boldsymbol{a}, \boldsymbol{b} \in \boldsymbol{H}$

(**Definition:** (G, ∗) be a group, H nonempty subset of G. H is a subgroup of G if H itself is a group under the same binary operation ∗)

Proof:

Necessary Part

Let (G, ∗) be a group. H is a nonempty subset of G.

Assume that H is a subgroup of G.

By definition, (H, ∗) is a group.

So $a, b \in H \Rightarrow b^{-1} \in H$ by inverse property

$\Rightarrow a * b^{-1} \in H$ by closure property

Sufficient Part

Let (G, ∗) be a group. H is a nonempty subset of G.

Assume $a, b \in H \Rightarrow a * b^{-1} \in H \rightarrow \quad (1)$

Claim: H is a subgroup of

G i.e., (H, ∗) is a group.

H is nonempty so let $a \in H$

(iii) Identity

Now $a, a \in H$ by (1)

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

i.e., $e \in H$

Identity exists

(iv)Inverse

Let a $\in H$. Now by previous step $e \in H$

Now $e, a \in H$ by (1)

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

$\Rightarrow e \in H$

Hence Inverse exists.

(i) Closure

Let $a, b \in H$ by previous step $b^{-1} \in H$

Now $a, b^{-1} \in H$ by (1)

$\Rightarrow a * (b^{-1})^{-1} \in H$

$\Rightarrow a * b \in H$

Closure is verified.

(ii) Associative

$a, b, c \in H$, $\boldsymbol{H \subseteq G}$, $a, b, c \in G$

In G $(a * b) * c = a * (b * c)$

$\therefore$ In H $(a * b) * c = a * (b * c)$

Associative is verified.

(H, $*$) be a group.

Hence H is a subgroup of G.

Hence the proof.

Theorem: 2

Prove that intersection of two subgroups of a group (G, $*$) is a subgroup of (G, $*$). Also, prove that union of subgroups need not be a group.

Proof:

Let (G, $*$) be a group. H and K are non – empty subgroups of (G, $*$). Both H and K satisfying the following necessary conditions

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

Let $a, b \in K \Rightarrow a * b^{-1} \in K$ . . . (1)

Consider the subset $H \cap K$ of G

(i) Since H is a subgroup of G, $e \in H$

Since K is a subgroup of G, $e \in K$

$\therefore e \in H \cap K$

so, $H \cap K$ is a non – empty subset of G.

(ii) Let a, b $\in H \cap K$

By Sufficient condition for aSubgroup

We need to prove $a * b^{-1} \in H \cap K$

$a, b \in H$ and $a, b \in K$

By (1) $a * b^{-1} \in H \cap K$

$\therefore H \cap K$ is a subgroup of (G, $*$)

Hence the proof.

Now we are going to Prove that Union of two Subgroups of a group need not be a Subgroup.

Let us prove the above fact by giving counter examples

Consider G = set of integers under addition $(Z, +)$

$= \{. . . , -3, -2, -1, 0, 1, 2, 3, . . . \}$

- $H = 2Z = \{. \ . \ . \ , \ -6, \ -4, \ -2, \ 0, \ 2, \ 4, \ 6, \ . \ . \ .\}$
- $K = 3Z = \{. \ . \ . \ , \ -9, \ -6, \ -3, \ 0, \ 3, \ 6, \ 9, \ . \ . \ .\}$

H and K are subgroups of $(Z, +)$

$H \cup K = \{. . . , -9, -6, -4, -3, -2, 0, 2, 3, 4, 6, 9, . . .\}$

$H \cup K$ is not closed under addition.

As $2,3 \in H \cup K$ but $2 + 3 = 5 \notin H \cup K$

So $H \cup K$ is not a subgroup of $(Z, +)$.

Hence the proof.

Cyclic Group:

Define Cyclic Groups

A group $(G, *)$ is said to be cyclic if there exists an element $a \in G$ such that every element of G can be written as some power of "a".

i.e., a^n *for some integer n.*

G is said to be generated by "a" (or) "a" is a generator ofG.

We write $G = \prec a \succ$

Examples:

The set of complex numbers $\{1, -1, i, -i\}$ under multiplication operation is a cyclic group.

There are two generators – i and i as $i^1 = 1$, $i^2 = -1$, $i^3 = -i$, $i^4 = 1$ and also $(-i)^1 = -i$, $(-i)^2 = -1$, $(-i)^3 = i$, $(-i)^4 = 1$ which covers all the elements of the group.

Hence it is a Cyclic Group.

However -1 is not a generator.

Theorem: 1

Every Subgroup of a Cyclic group is Cyclic.

Proof:

Let H be a cyclic group generated by an element $a \epsilon G$.

∴ Every element in G can be expressed as a power of the element "a".

Let H be a subgroup of G.

If $H = \{e\}$, then H is a subgroup of G and it is cyclic.

∴ The result is trivial.

Suppose $H \neq \{e\}$ then there exists an element $x \epsilon H$ with $x \neq e$.

$\therefore x = a^k$ for some integer k.

Let m be the least positive integer such that $a^m \epsilon H$.

Let $b \epsilon H$ then $b = a^n$ for some integer n.

Let $n = mq + r$ where $0 \leq r < m$

$\Rightarrow b = a^n$

$\Rightarrow b = a^{mq+r}$

$\Rightarrow b = a^{mq} * a^r$

$\Rightarrow b = (a^m)^q * a^r$

$\Rightarrow a^r = b/(a^m)^q$

$\Rightarrow a^r = b * (a^m)^{-q}$

Now $b \epsilon H$, $(a^m)^q \epsilon H$ and H is closed in $*$.

$\therefore$ we have $b * (a^m)^{-q} \epsilon H$

This shows that there exists an integer "r" such that $o \leq r < m$ with $a^r \epsilon H$.

Since m is the least positive integer for which $a^m \epsilon H$, $a^r \epsilon H$ with $o \leq r < m$ is not possible.

$\therefore r = 0$ so $b = a^{mq}$

$\Rightarrow b = (a^m)^q$

Every element $b \epsilon H$ is expressed as a power of a^m.

i.e., H is generated by the element $a^m \epsilon H$

H is a cyclic group generated by a^m.

Hence, every subgroup of a cyclic group is

cyclic.

Hence the proof.