SUBGROUPS

Shahzad Ahmad Khan
Lecturer (Mathematics)
Govt.College Kot Sultan
District Layyah.

Subgroup

Let $(G, \bullet)$ be a group and H be a non-empty subset of G. If H is itself a group with the same binary operation defined on G, then H is called a subgroup of G.

Examples $(Z, +)$ is a subgroup of $(Q, +)$

$(Q, +)$ is a subgroup of $(R, +)$

Trivial and Non-trivial Subgroups

Every group G has at least two subgroups namely G itself and the identity group $\{e\}$. These are called *trivial subgroups*. Any other subgroup of G is called non-trivial subgroup of G.

Example Here $G = \{1, -1, i, -i\}$ is a group under multiplication.

Trivial subgroup of group G are $\{e\}$ and G itself.

Non-trivial subgroup of G is only $\{1, -1\}$

Theorem

Let $(G, \bullet)$ be a group. A non-empty subset H of G is a subgroup of G if and only if for all $a, b \in H$, the element $ab^{-1} \in H$

Proof:

Let G be a group and $H \subseteq G$ further $H \neq \phi$. We are to prove that

$$H \text{ is a subgroup of } G \Leftrightarrow a, b \in H \Rightarrow ab^{-1} \in H$$

Suppose H is a subgroup of G, then H is itself a group.

Let $a, b \in H \Rightarrow a, b^{-1} \in H$ $\because$ H is a group.

$\Rightarrow ab^{-1} \in H$ $\because$ H is a group.

Conversely suppose that $a, b \in H \Rightarrow ab^{-1} \in H$ ..... (1)

We shall prove that H is a subgroup of G

Since $H \subseteq G$ $\therefore$ we shall only prove that H is a subgroup of G.

(I) Identity Property

We shall prove that $e \in H$

Let $a \in H$

Since $a, a \in H \Rightarrow aa^{-1} \in H$ [By (1)]

$\Rightarrow e \in H$

(II) Inverse Property

Let $a \in H$, we shall prove that $a^{-1} \in H$

Since $e, a \in H \Rightarrow ea^{-1} \in H$ [By (1)]

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

(III) Closure Property

Let $a, b \in H$. we are to prove that $ab \in H$

Since $a, b \in H \Rightarrow a, b^{-1} \in H$ [By Inverse Property]

$\Rightarrow a(b^{-1})^{-1} \in H$ [By (1)]

$\Rightarrow ab \in H$ [$\because (b^{-1})^{-1} = b$]

(IV) Associative Property

Since G is a group.

$\therefore$ if $x, y, z \in G$ then $(xy)z = x(yz)$

Let $a, b, c \in H$ then $(ab)c = a(bc)$ $\because H \subseteq G$

From (I), (II), (III) and (IV), H is a group.

Theorem

The intersection of any collection of subgroups of a group G is a subgroup of G.

Proof:

Let $\{H_i : i \in I\}$ be a collection of subgroups of a group G.

Let $\cap \{H_i : i \in I\} = H$. We shall prove that H is a subgroup of G.

Let $a, b \in H \Rightarrow a, b \in \cap \{H_i : i \in I\}$

$\Rightarrow a, b \in H_i ; \forall i$

$\Rightarrow ab^{-1} \in H_i ; \forall i$ $\because$ Each H_i is a subgroup.

$\Rightarrow ab^{-1} \in \cap \{H_i : i \in I\}$

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

Thus H (The collection of subgroups) is a subgroup of group G.

Theorem

Let G be a group and H a subgroup of G. Then the set $aHa^{-1} = \{aha^{-1} : h \in H\}$ is a subgroup of G.

Proof:

Let $x, y \in aHa^{-1}$. we shall prove that $xy^{-1} \in aHa^{-1}$

Here $x = ah_1a^{-1}$ and $y = ah_2a^{-1}$; $h_1, h_2 \in H$

Now, $xy^{-1} = (ah_1a^{-1})(ah_2a^{-1})^{-1}$

$= ah_1a^{-1}.ah_2^{-1}a^{-1}$ $\because (abc)^{-1} = c^{-1}b^{-1}a^{-1}$

$= ah_1(a^{-1}a)h_2^{-1}a^{-1}$

$= ah_1eh_2^{-1}a^{-1}$

$= ah_1h_2^{-1}a^{-1}$

Since H is a subgroup and $h_1, h_2 \in H \quad \therefore h_1h_2^{-1} \in H$

So, $xy^{-1} = ah_1h_2^{-1}a^{-1} \in aHa^{-1}$

Hence aHa^{-1} is a subgroup of G.

Remark

For two subgroups H, K of a group G, their union $H \cup K$ need not be a subgroup of G.

For example $G = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ is a group under multiplication modulo 8.

Also $H = \{\bar{1}, \bar{3}\}$, $K = \{\bar{1}, \bar{5}\}$ are both subgroups of G.

Note that $H \cup K = \{\bar{1}, \bar{3}, \bar{5}\}$ is not a subgroup of $G \quad \because \bar{3}.\bar{5} = \bar{7} \notin H \cup K$

Theorem

The union $H \cup K$ of two subgroups H and K of a group G is a subgroup of G if and only if either $H \subset K$ or $K \subset H$.

Proof:

are subgroups

Let G be a group and H and K of a group G. We are to prove that

$H \cup K$ is a subgroup of $G \Leftrightarrow$ either $H \subset K$ or $K \subset H$.

Suppose that $H \cup K$ is a subgroup of G.

We have to prove that either $H \subset K$ or $K \subset H$.

We suppose the contrary that $H \not\subset K$ and $K \not\subset H$

If $H \not\subset K$ then let $a \in H$ and $a \notin K$

If $K \not\subset H$ then let $b \in K$ and $b \notin H$

Since $a \in H, b \in K \Rightarrow a, b \in H \cup K$

$\Rightarrow ab \in H \cup K \quad \because H \cup K$ is a subgroup

$\Rightarrow ab \in H$ Or $ab \in K$

When $ab \in H$

Since $a \in H \quad \therefore a^{-1} \in H \quad \because H$ is a subgroup.

Now $b = a^{-1}(ab) \in H \quad \because H$ is a subgroup.

When $ab \in K$

Since $b \in K \quad \therefore b^{-1} \in K \quad \because K$ is a subgroup.

Now $a = (ab)b^{-1} \in K \quad \because K$ is a subgroup.

Hence $b \in H$ or $a \in K$ which is contradiction to our supposition.

Hence $H \not\subset K$ and $K \not\subset H$ is wrong. Thus $H \subset K$ or $K \subset H$.

Conversely suppose that $H \subset K$ or $K \subset H$.

We are to prove that $H \cup K$ is a subgroup of G.

Now $H \subset K \Rightarrow H \cup K = K$ (subgroup)

Or $K \subset H \Rightarrow H \cup K = H$ (subgroup)

Since H and K are subgroup of G, $\therefore$ $H \cup K$ is a subgroup of G.

Remark

(i) Every element of a group G can generate a subgroup of G.

(ii) If G is group and $O(G) = n$. Let $a \in G$ then $H = \{a^k : k \in Z^+\}$ is a subgroup of G.

Example

Find the subgroups of group $G = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ with the following addition table.

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

Solution

Here the binary operation is addition modulo 4 with $\bar{0}$ as an identity element.

Let $H_1 = \{\bar{0}\}$

$H_2 = \{(\bar{1})^1 = \bar{1}, (\bar{1})^2 = \bar{2}, (\bar{1})^3 = \bar{3}, (\bar{1})^4 = \bar{0}\} = \{\bar{1}, \bar{2}, \bar{3}, \bar{0}\} = \langle \bar{1} : (\bar{1})^4 = \bar{0} \rangle$

$H_3 = \{(\bar{2})^1 = \bar{2}, (\bar{2})^2 = \bar{0}\} = \{\bar{2}, \bar{0}\} = \langle \bar{2} : (\bar{2})^2 = \bar{0} \rangle$ — symbol of cyclic

$H_4 = \{(\bar{3})^1 = \bar{3}, (\bar{3})^2 = \bar{2}, (\bar{3})^3 = \bar{1}, (\bar{3})^4 = \bar{0}\} = \{\bar{3}, \bar{2}, \bar{1}, \bar{0}\} = \langle \bar{3} : (\bar{3})^4 = \bar{0} \rangle$

Trivial subgroups of G are $\{\bar{0}\}$ and $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}\} = G$

Non-trivial subgroup of G is $\{\bar{0}, \bar{2}\}$

Example

Find the subgroups of the group $G = \{e, a, b, c\}$ defined by

$+$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Solution

Here $G = \{e, a, b, c\}$ is a group such that

$a^2 = b^2 = c^2 = e$ (It is clear from the table)

Let $H_1 = \{e\}$

$H_2 = \{a^1, a^2 = e\} = \{a, e\} = \langle a : a^2 = e \rangle$

$H_3 = \{b^1, b^2 = e\} = \{b, e\} = \langle b : b^2 = e \rangle$

$H_4 = \{c^1, c^2 = e\} = \{c, e\} = \langle c : c^2 = e \rangle$

Trivial subgroups of G are $\{e\}$ and G

Non-trivial subgroups of G are $\{a, e\}, \{b, e\}$ and $\{c, e\}$

Example

Let $C - \{0\}$ be the group of all non-zero complex numbers under multiplication. Prove that the set $H = \{a + ib \in C - \{0\} : a^2 + b^2 = 1\}$ is a subgroup of $C - \{0\}$.

Solution

Let $a_1 + ib_1, a_2 + ib_2 \in H$, so that $a_1{}^2 + b_1{}^2 = 1$ and $a_2{}^2 + b_2{}^2 = 1$

Now $(a_1 + ib_1)(a_2 + ib_2)^{-1} = \frac{a_1+ib_1}{a_2+ib_2}$

$= \frac{a_1+ib_1}{a_2+ib_2} \times \frac{a_2-ib_2}{a_2-ib_2}$

$= \frac{(a_1+ib_1)(a_2-ib_2)}{a_2{}^2+b_2{}^2}$

$= \frac{(a_1a_2+b_1b_2)+i(a_2b_1-a_1b_2)}{1}$ $[\because a_2{}^2 + b_2{}^2 = 1]$

$= (a_1a_2 + b_1b_2) + i(a_2b_1 - a_1b_2)$

Here $(a_1a_2 + b_1b_2)^2 + (a_2b_1 - a_1b_2)^2 = a_1{}^2a_2{}^2 + b_1{}^2b_2{}^2 + a_2{}^2b_1{}^2 + a_1{}^2b_2{}^2$

$= a_1{}^2(a_2{}^2 + b_2{}^2) + b_1{}^2(a_2{}^2 + b_2{}^2)$

$= (a_1{}^2 + b_1{}^2)(a_2{}^2 + b_2{}^2)$

$= 1.1$

$= 1$

Thus $(a_1 + ib_1)(a_2 + ib_2)^{-1} \in H$

This shows that H is a subgroup of $C - \{0\}$

Cyclic Groups

Cyclic Group

A group G is said to be cyclic if there exist an element $a \in G$ such that every element of G can be written in the form of $a^k; k \in Z$

The group G is then written as $G = \langle a \rangle$, while "a" is called generator of G. If order of "a" is "n" (*i.e.* $a^n = e$) then G is said to be cyclic group of order n.

Then the group G is written as $G = \langle a : a^n = e \rangle$

Example

Since $G = \{1, -1, i, -i\}$ is a group under "."

Note that $i \in G$ and $(i)^1 = i$

$(i)^2 = -1$

$(i)^3 = i^2.i = (-1).i = -i$

$(i)^4 = i^2.i^2 = (-1)(-1) = 1$

Every element of G can be written in the form of i^k : $k = 1,2,3,4$

Further $i^4 = 1$, $\therefore$ G is cyclic group generated by i and $G = \langle i : i^4 = 1 \rangle$

Theorem ✗

Every subgroup of a cyclic group is cyclic.

Proof:

Let G be a cyclic group generated by a then every element of G will be of the form a^i, $i \in Z$

Let H be a subgroup of G, then every element of H is also of the form a^i, $i \in Z$

Suppose k is the smallest positive integer such that a^k, $k \in Z$

We are to prove that H is cyclic group generated by a^k, $k \in Z$

i.e. we are to prove that every element of H is of the form $(a^k)^i$, $i \in Z$

Let $a^m \in H$ we have to prove that $a^m = (a^k)^i$, $i \in Z$

Since $k < m$ then by Euclid's Theorem, there exists unique integer q, r such that $m = kq + r$, $0 \leq r < k$

Now $a^m = a^{kq+r}$

$\Rightarrow$ $a^m = a^{kq}.a^r$

$\Rightarrow$ $a^{-kq}.a^m = a^r$

$\Rightarrow ((a^k)^q)^{-1}.a^m = a^r$.... (1)

Since $a^k \in H$ $\Rightarrow$ $(a^k)^q \in H$ $\because$ H is a subgroup of G.

$\Rightarrow ((a^k)^q)^{-1} \in H$ $\because$ H is a subgroup of G.

Again $a^m, ((a^k)^q)^{-1} \in H$ $\Rightarrow$ $a^m.((a^k)^q)^{-1} \in H$ $\because$ H is a subgroup of G.

$\Rightarrow a^r \in H$ [By (1)]

Thus $a^r \in H$, $0 \leq r < k$; this is contradiction unless $r = 0$

Now, $a^m = a^{kq+r}$

$= a^{kq}$ $\because$ r = 0

$= (a^k)^q$ Where $q \in Z$

Hence the proof.

Theorem

Let G be a cyclic group of order n generated by a. Then for each positive divisor d of n, there is a unique subgroup (of G) of order d.

Proof:

Let $G = \langle a : a^n = e \rangle$

Let d be a positive divisor of n.

Then $d = 1$ or $d = n$ or $1 < d < n$

If $d = 1$ then, subgroup of G of order 1 is $\{e\}$

If $d = n$ then, subgroup of G of order n is G itself

Further $\{e\}$ and G are unique.

If $1 < d < n$ then let $\frac{n}{d} = q \Rightarrow qd = n,\ q \in Z$

Since $e = a^n = a^{qd} = (a^q)^d$

Let $H = \langle a^q : (a^q)^d = e \rangle$ where $a^q \in G$

Thus H is a subgroup of G of order d.

[$\because$ If G is a group and $a \in G$ then "a" can generate a subgroup of G]

Uniqueness

Suppose k is another subgroup of G of order d.

Let $K = \langle a^k : (a^k)^d = e \rangle$, where $a^k \in G$

Now, $a^{kd} = e = a^n \Rightarrow kd = n$

$\Rightarrow k = \frac{n}{d} = q$

Hence $q = k$

$\Rightarrow a^q = a^k$

$\Rightarrow H = K$

Theorem

Prove that every cyclic group is abelian.

Proof:

Let G be a cyclic group generated by a, then every element of G can be written in the form of $a^i,\ i \in Z$

Let $x, y \in G$ then $x = a^m,\ m \in Z$

& $y = a^k,\ k \in Z$

Now $xy = a^m a^k$

$= a^{m+k}$

$= a^{k+m}$

$= a^k a^m$

$= yx$

Since $xy = yx\ \forall\ x, y \in G \Rightarrow G$ is an abelian group.

Theorem

If G is a cyclic group of even order, then prove that there is only one subgroup of order 2 in G.

Proof:

Let $G = \langle a : a^{2n} = e \rangle$ be a cyclic group of order $2n$, where n is a positive integer.

We know that if a positive integer d divides $O(G)$ then G has exactly one subgroup of order d.

Now $O(G) = 2n$ and 2 divides $2n$, so G has only one subgroup of order 2.

Example

Find all the subgroups of a cyclic group of order 12.

Solution

Let $G = \langle a : a^{12} = e \rangle$

All the positive divisors of 12 are 1,2,3,4,6,12.

Thus there are six subgroups of G of orders 1,2,3.4,6,12.

The generators of these subgroups are $a^{12} = e, a^6, a^4, a^3, a^2, a^1$

Let $H_1 = \{e\}$

$H_2 = \langle a^6 : (a^6)^2 = e \rangle = \{(a^6)^1, (a^6)^2 = e\} = \{a^6, e\}$

$H_3 = \langle a^4 : (a^4)^3 = e \rangle = \{(a^4)^1, (a^4)^2, (a^4)^3 = e\} = \{a^4, a^8, e\}$

$H_4 = \langle a^3 : (a^3)^4 = e \rangle = \{(a^3)^1, (a^3)^2, (a^3)^3, (a^3)^4 = e\} = \{a^3, a^6, a^9, e\}$

$H_5 = \langle a^2 : (a^2)^6 = e \rangle = \{(a^2)^1, (a^2)^2, (a^2)^3, (a^2)^4, (a^2)^5, (a^2)^6 = e\}$

$= \{a^2, a^4, a^6, a^8, a^{10}, e\}$

$H_6 = \langle a : a^{12} = e \rangle = G$

COSETS AND LAGRANGE'S THEOREM

Coset

Let H be a subgroup of G and $a \in G$, then the set

$$aH = \{ ah : h \in H \}$$

is called left coset of H in G determined by a.

Similarly the set $Ha = \{ ha : h \in H \}$ is called right coset of H in G determined by a.

If H is a subgroup of the group $(G, +)$ then left coset of H in G determined by a is $a + H = \{ a + h : h \in H \}$

Example

Let $G = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ be a group under addition modulo 6. Let $H = \{\bar{0}, \bar{2}, \bar{4}\}$ be a subgroup of G. Find all left coset of H in G.

Solution

Here
$$\bar{0} + H = \{\bar{0} + \bar{0}, \bar{0} + \bar{2}, \bar{0} + \bar{4}\} = \{\bar{0}, \bar{2}, \bar{4}\}$$
$$\bar{1} + H = \{\bar{1} + \bar{0}, \bar{1} + \bar{2}, \bar{1} + \bar{4}\} = \{\bar{1}, \bar{3}, \bar{5}\}$$
$$\bar{2} + H = \{\bar{2} + \bar{0}, \bar{2} + \bar{2}, \bar{2} + \bar{4}\} = \{\bar{2}, \bar{4}, \bar{0}\}$$
$$\bar{3} + H = \{\bar{3} + \bar{0}, \bar{3} + \bar{2}, \bar{3} + \bar{4}\} = \{\bar{3}, \bar{5}, \bar{1}\}$$
$$\bar{4} + H = \{\bar{4} + \bar{0}, \bar{4} + \bar{2}, \bar{4} + \bar{4}\} = \{\bar{4}, \bar{0}, \bar{2}\}$$
$$\bar{5} + H = \{\bar{5} + \bar{0}, \bar{5} + \bar{2}, \bar{5} + \bar{4}\} = \{\bar{5}, \bar{1}, \bar{3}\}$$

Thus there are two left cosets in G, $\{\bar{0}, \bar{2}, \bar{4}\}$ and $\{\bar{1}, \bar{3}, \bar{5}\}$

Example

Let $G = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ be a group under multiplication modulo 8. Let $H_1 = \{\bar{1}, \bar{3}\}$, $H_2 = \{\bar{1}, \bar{5}\}$, $H_3 = \{\bar{1}, \bar{7}\}$ be a subgroups of G. Find all left coset of H_1 in G.

Solution

Here
$$\bar{1}.H_1 = \{\bar{1}.\bar{1}, \bar{1}.\bar{3}\} = \{\bar{1}, \bar{3}\}$$
$$\bar{3}.H_1 = \{\bar{3}.\bar{1}, \bar{3}.\bar{3}\} = \{\bar{3}, \bar{1}\}$$
$$\bar{5}.H_1 = \{\bar{5}.\bar{1}, \bar{5}.\bar{3}\} = \{\bar{5}, \bar{7}\}$$
$$\bar{7}.H_1 = \{\bar{7}.\bar{1}, \bar{7}.\bar{3}\} = \{\bar{7}, \bar{5}\}$$

Thus left cosets of H in G are $\{\bar{1}, \bar{3}\}$ and $\{\bar{5}, \bar{7}\}$

Note

(i) Any two left (or right) cosets of H in G will be equal or disjoint.

(ii) If G is abelian then $aH = Ha$ for some $a \in G$

Partition of a set

Let $A_1, A_2, A_3, \ldots\ldots\ldots, A_n$ be a collection of subsets of a set A, then this collection form a partition of A if

(i) $\cup \{A_i : i \in I\} = A$ and (ii) $A_i \cap A_j = \phi$

Theorem

Let H be a subgroup of G, then the set of all left (or right) cosets of H in G defines a partition of G.

Proof:

Let $A = \{aH : a \in G\}$ be a collection of all distinct left cosets of H in G.

We shall prove that (i) $\cup \{aH : a \in G\} = G$ (ii) $aH \cap bH = \phi$

(i) To prove $\cup \{aH : a \in G\} = G$ we have to show that

$$G \subseteq \cup \{aH : a \in G\} \text{ and } \cup \{aH : a \in G\} \subseteq G$$

$$(\because A = B \Leftrightarrow A \subseteq B, B \subseteq A)$$

Let $a \in G$ then $a = ae \in aH \subseteq \cup \{aH : a \in G\}$

Because $a \in G \Rightarrow a \in \cup \{aH : a \in G\}$. Thus $G \subseteq \cup \{aH : a \in G\}$ ..... (1)

Since $aH \subseteq G;\ \forall\, a \in G.\ \therefore \cup\{aH : a \in G\} \subseteq G$ ..... (2)

From (1) and (2) we get $\cup\{aH : a \in G\} = G$

(ii) Let $aH, bH \in A$ Then $aH \neq bH$

We have to prove that $aH \cap bH = \phi$

We assume the contrary that $aH \cap bH \neq \phi$

Let $x \in aH \cap bH \Rightarrow x \in aH$ and $x \in bH$

$\Rightarrow x = ah_1$ and $x = bh_2$ Where $h_1, h_2 \in H$

$\Rightarrow ah_1 = bh_2$

$\Rightarrow a = (bh_2){h_1}^{-1}$

$\Rightarrow a = b(h_2{h_1}^{-1})$

$\Rightarrow a = bh_3$ Where $h_3 = h_2{h_1}^{-1} \in H$

$\Rightarrow b = a{h_3}^{-1}$ Where ${h_3}^{-1} \in H$

Now for these values of a and b we can prove that $aH = bH$

Let $y \in aH$	Let $y \in bH$
$\Rightarrow y = ah_4$ where $h_4 \in H$	$\Rightarrow y = bh_6$ where $h_6 \in H$
$\Rightarrow y = (bh_3)h_4$ $\because a = bh_3$	$\Rightarrow y = (a{h_3}^{-1})h_6$ $\because b = a{h_3}^{-1}$
$\Rightarrow y = b(h_3h_4)$ By associative Law	$\Rightarrow y = a({h_3}^{-1}h_6)$ By associative Law
$\Rightarrow y = bh_5 \in bH$ $\because h_5 = h_3h_4 \in H$	$\Rightarrow y = ah_7 \in aH$ $\because h_7 = {h_3}^{-1}h_6 \in H$
Thus $aH \subseteq bH$ ..... (*)	Thus $bH \subseteq aH$ ..... (**)

By (*) and (**) we get $aH = bH$ which is contradiction.

Thus $aH \cap bH = \phi$ This completes the proof.

Index of Subgroup in Group

The number of distinct left (or right) cosets of a subgroup H of a group G is called the index of H in G.

Example

Find the distinct left (or right) cosets of

$$E = \{0, \pm 2, \pm 4, \ldots\} = \{2n : n \in Z\}$$

in the group $(Z, +)$.

Solution

The only left cosets of E in Z are $0 + E$ and $1 + E$

Here $0 + E = \{0 + 2n : n \in Z\} = E$

$1 + E = \{1 + 2n : n \in Z\}$

$= \{\pm 1, \pm 2, \pm 3\}$

and $E \cup \{1 + E\} = Z,\ E \cap \{1 + E\} = \varphi$

Therefore, the index of E in Z is 2.

Lagrange's Theorem

The order and index of a subgroup of a finite group divide the order of the group.

Proof:

Let H be a subgroup of a finite group G.

Let $O(G) = n$, $O(H) = m$, and $[G:H] = k$

Let A be a collection of all left cosets of H in G, then

$$A = \{ a_1H, a_2H, a_3H, \ldots\ldots, a_kH \}$$

We know that this collection defines a partition of G.

i.e. **(i)** $G = a_1H \cup a_2H \cup a_3H \cup \ldots\ldots \cup a_kH$ and **(ii)** $a_iH \cap a_jH = \phi$

Thus, $O(G) = O(a_1H) + O(a_2H) + O(a_3H) + \ldots\ldots + O(a_kH) \ldots\ldots\ldots$ **(1)**

First we shall prove that $O(H) = O(a_iH)$

Now $O(H) = O(a_iH)$ if $\exists$ a bijective function from H to a_iH

We define $f: H \to a_iH$ as $f(h) = a_ih$; $\forall\, h \in H$

f is one-one function

Let $h_1, h_2 \in H$ such that $f(h_1) = f(h_2)$

$\Rightarrow \quad a_ih_1 = a_ih_2$

$\Rightarrow \quad h_1 = h_2$ [By Cancellation Law]

$\Rightarrow$ f is one-one function.

f is onto function

Let $a_ih \in a_iH$ then $h \in H$ and $f(h) = a_ih$

Hence f is onto function also.

Since f is one-one and onto, therefore f is a bijective function.

Therefore, $O(H) = O(a_iH)$

Thus **(1)** $\Rightarrow$ $O(G) = O(H) + O(H) + O(H) + \ldots\ldots\ldots + O(H)$ [k- times]

$\Rightarrow \quad n = m + m + m + \ldots\ldots\ldots + m$ [k- times]

$\Rightarrow \quad n = km$

$\Rightarrow \quad m|n$ and $k|n$ [$\because$ If $a = bc$ then $b|a, c|a$]

$\Rightarrow \quad O(H)|O(G)$ and $[G:H]|O(G)$

Theorem

The order of an element of a finite group divides the order of the group.

Proof:

Let G be a group and $O(G) = n$,

Let $a \in G$ such that $O(a) = k$ i.e. $a^k = e$

Let $H = \langle a : a^k = e \rangle$, then H is a subgroup of G of order k

We know by Lagrange's Theorem that $O(H)|O(G)$

$\Rightarrow \quad O(a)|O(G) \quad \because\ O(H) = O(a) = k$

Theorem

Prove that a group G whose order is prime number is necessarily cyclic.

Proof:

Let G be a group such that $O(G) = p$, where p is a prime number.

We are to prove that G is a cyclic group.

Let $H = \langle a : a^m = e \rangle$

Then H is a subgroup of G of order m.

($\because$ Every element of G can generate a subgroup of G)

Then by Lagrange's Theorem we get

$O(H) | O(G) \Rightarrow m | p$ This is possible only when if $m = p$ or $m = 1$

But $m \neq 1 \quad \because H \neq \{e\}$

$\therefore \quad m = p$

Hence $O(H) = p = O(G)$

Therefore, $H = G = \langle a : a^m = e \rangle$

Thus is G a cyclic group.

EXERCISE 2.2

Q. No.1

Give an example of an abelian group which is not cyclic.

Solution

Let $G = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$

Then G is group under multiplication modulo 8.

$\bullet$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{1}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{7}$	$\bar{5}$
$\bar{5}$	$\bar{5}$	$\bar{7}$	$\bar{1}$	$\bar{3}$
$\bar{7}$	$\bar{7}$	$\bar{5}$	$\bar{3}$	$\bar{1}$

G is abelian

$\because ab = ba \ \forall \ a, b \in G.$

G is not cyclic

Since $(\bar{3})^2 = \bar{1} \Rightarrow O(\bar{3}) = 2$

$(\bar{5})^2 = \bar{1} \Rightarrow O(\bar{5}) = 2$

$(\bar{7})^2 = \bar{1} \Rightarrow O(\bar{7}) = 2$

But $O(G) = 4$

Now G is not cyclic because every element of G can't written in the power of one and the same element.

Since, order of every element of G < order of G

Therefore no element of G can generate a subgroup of G.

Hence G is not cyclic.

Q. No.2

Explain why a group of order 47 cannot have proper subgroups?

Solution

We know by Lagrange's Theorem that the order of a subgroup divides the order of the group.

Let G be a group of order 47.

Since 47 is a prime number so 47 has only two divisors 1 and 47.

So, we have only two subgroups of G of orders $m = 1$ and $m = 47$

When $m = 1$, $H = \{e\}$, (which is an improper (trivial) subgroup of G.)

When $m = 47, H = G$, (which is also an improper (trivial) subgroup of G.)

This shows that G have no proper subgroups.

Q. No.3

Let G be a group of order 89. Can G have a subgroup of
(i) order 12 (ii) order 16. (iii) order 24? Justify your answer.

Solution

We know by Lagrange's Theorem that the order of a subgroup divides the order of the group.

Since 12,16 or 24 cannot divide 89.

This shows that group of order 89 cannot have subgroups of orders 12,16 or 24.

Q. No. 4

Show that an infinite cyclic group has exactly two distinct generators.

Solution

Let G be an infinite cyclic group then $\exists\ a \in G$ such that

$$G = \{ a^m : m \in Z \} \quad \ldots\ldots\ldots \quad (1)$$

Now $a^m = (a^{-1})^{-m}$

Then (1) $\Rightarrow\ G = \{ (a^{-1})^{-m} : m \in Z \}$

$\Rightarrow\ a^{-1}$ is a generator of G.

Thus if a is a generator of G then a^{-1} is also a generator of G.

Hence G has at least two generators.

Suppose $c \in G$ is also a generator of G.

i.e. $G = \{ c^k : k \in Z \}$

Since $a \in G \quad \therefore\ \exists\ m_1 \in Z$ such that $c^{m_1} = a$ ..... (2)

Also $G = \{ a^m : m \in Z \}$

Since $c \in G \quad \therefore\ \exists\ m_2 \in Z$ such that $a^{m_2} = c$ ..... (3)

Putting the value of c from (3) in (2)

We get, $(a^{m_2})^{m_1} = a$

$\Rightarrow\ a^{m_1 m_2} = a$

$\Rightarrow\ m_1 m_2 = 1$

$\Rightarrow\ m_1 = m_2 = 1$ or $m_1 = m_2 = -1$

Put $m_1 = 1$ in equation (2), we get $c = a$

Put $m_2 = -1$ in equation (3), we get $c = a^{-1}$

Hence $c = a$ or $c = a^{-1}$

Thus G has exactly two distinct generators.

If Q is cyclic gp generated by a then $a = \frac{p}{q}$, $q \neq 0$ and each element of Q must be expressed in the form $\{a, 2a, 3a \ldots\}$ i.e. multiples

Q. No. 5

Is $(Q, +)$ a cyclic group? Why?

Solution

Consider the group $(Q, +)$.

If Q is a cyclic group then each $x \in Q$ must be generated by a single element $a \in Q$.

i.e. Each $x \in Q$ must be of the form $x = na$ for some $n \in Z$

Here $\frac{a}{2} \in Q$ is not of the form na, $n \in Z$

$\because$ If $\frac{a}{2}$ is of the form na, $n \in Z$

Then $\frac{a}{2} = na$, $n \in Z$

But $n = \frac{1}{2} \notin Z$

$\therefore$ $\frac{a}{2} \in Q$ is not generated by $a \in Q$ under the binary operation "+".

Thus $(Q, +)$ is not a cyclic group.

Q. No.6

Let G be a cyclic group of order 24 generated by a. Find the orders of the elements (i) e (ii) a^9 (iii) a^{10}

Solution

Since G be a cyclic group of order 24 generated by a

So, $G = \langle a : a^{24} = e \rangle$

(i) $O(e) = ?$

Let $O(e) = m$ then $a^m = e$, where m is the least +ive integer.

$\Rightarrow$ $m = 1$

(ii) $O(a^9) = ?$

Let $O(a^9) = m$ then $(a^9)^m = e$, where m is the least +ive integer.

$\Rightarrow$ $a^{9m} = e$

We know that if $O(a) = m$ and $a^n = e$ then $m|n$

Here $O(a) = 24$ and $a^{9m} = e$

$\therefore$ $24|9m$

$\Rightarrow$ $9m = 24k$ Where $k \in Z$

$\Rightarrow$ $m = \frac{8}{3}k$

For least positive integral value of m, we take $k = 3$

$\therefore$ $m = 8$ i.e. $O(a^9) = 8$

(iii) $O(a^{10}) = ?$

Let $O(a^{10}) = m$ then $(a^{10})^m = e$, where m is the least +ive integer.

$\Rightarrow$ $a^{10m} = e$

We know that if $O(a) = m$ and $a^n = e$ then $m|n$

Here $O(a) = 24$ and $a^{10m} = e$

$\therefore$ $24|10m$

$\Rightarrow$ $10m = 24k$ Where $k \in Z$

$\Rightarrow$ $m = \frac{12}{5}k$

For least positive integral value of m, we take $k = 5$

$\therefore$ $m = 12$ i.e. $O(a^{10}) = 12$

Q. No.7

Find all the subgroups of a cyclic group of order 60 generated by a.

Solution

Let $G = \langle a : a^{60} = e \rangle$

All the positive divisors of 60 are 1,2,3,4,5,6,10,12,15,20,30,60.

Thus there are six subgroups of G of orders 1,2,3,4,5,6,10,12,15,20,30,60.

The generators of these subgroups are

$a^{60} = e, , a^{30}, a^{20}, a^{15}, a^{12}, a^{10}, a^6, a^5, a^4, a^3, a^2, a^1$

Let $H_1 = \{e\}$

$H_2 = \langle a^{30} : (a^{30})^2 = e \rangle = \{(a^{30})^1, (a^3)^2 = e\} = \{a^{30}, e\}$

$H_3 = \langle a^{20} : (a^{20})^3 = e \rangle = \{(a^{20})^1, (a^{20})^2, (a^{20})^3 = e\} = \{a^{20}, a^{40}, e\}$

$H_4 = \langle a^{15} : (a^{15})^4 = e \rangle = \{(a^{15})^1, (a^{15})^2, (a^{15})^3, (a^{15})^4 = e\}$

$= \{a^{15}, a^{30}, a^{45}, e\}$

$H_5 = \langle a^{12} : (a^{12})^5 = e \rangle = \{(a^{12})^1, (a^{12})^2, (a^{12})^3, (a^{12})^4, (a^{12})^5 = e\}$

$= \{a^{12}, a^{24}, a^{36}, a^{48}, e\}$

$H_6 = \langle a^{10} : (a^{10})^6 = e \rangle$

$H_7 = \langle a^6 : (a^6)^{10} = e \rangle$

$H_8 = \langle a^5 : (a^5)^{15} = e \rangle$

$H_9 = \langle a^4 : (a^4)^{15} = e \rangle$

$H_{10} = \langle a^3 : (a^3)^{20} = e \rangle$

$H_{11} = \langle a^2 : (a^2)^{30} = e \rangle$

$H_{12} = \langle a : a^{60} = e \rangle = G$

Q. No.8

Find all the subgroups of a cyclic group of order 18.

Solution

Let $G = \langle a : a^{18} = e \rangle$

All the positive divisors of 18 are 1,2,3,6,9,18.

Thus there are six subgroups of G of orders 1,2,3,6,9,18.

The generators of these subgroups are $a^{18} = e, , a^9, a^6, a^3, a^2, a^1$

Let $H_1 = \{e\}$

$H_2 = \langle a^9 : (a^9)^2 = e \rangle = \{(a^9)^1, (a^9)^2 = e\} = \{a^9, e\}$

$H_3 = \langle a^6 : (a^6)^3 = e \rangle = \{(a^6)^1, (a^6)^2, (a^6)^3 = e\} = \{a^6, a^{12}, a^{18} = e\}$

$H_4 = \langle a^3 : (a^3)^6 = e \rangle = \{(a^3)^1, (a^3)^2, (a^3)^3, (a^3)^4, (a^3)^5, (a^3)^6 = e\}$

$= \{a^3, a^6, a^9, a^{12}, a^{15}, e\}$

$H_5 = \langle a^2 : (a^2)^9 = e \rangle$

$= \{(a^2)^1, (a^2)^2, (a^2)^3, (a^2)^4, (a^2)^5, (a^2)^6, (a^2)^7, (a^2)^8, (a^2)^9 = e\}$

$= \{a^2, a^4, a^6, a^8, a^{10}, a^{12}, a^{14}, a^{16}, e\}$

$H_6 = \langle a : a^{18} = e \rangle = G$

Q. No.9

Let H be the set of real numbers of the form $a + b\sqrt{2}$, where $a, b \in Q$ and both are not simultaneously zero. Show that H is a subgroup of the group of non-zero real numbers under multiplication. $R - \{0\}$

Solution

Let $H = \{a + b\sqrt{2} : a, b \in Q\}$ where a, b are not simultaneously zero.

We are to prove that $(H,\bullet)$ is a subgroup of the group $(R - \{0\},\bullet)$.

Let $x, y \in H$

Then $x = a_1 + b_1\sqrt{2}$ where $a_1, b_1 \in Q$ and are not simultaneously zero.

And $y = a_2 + b_2\sqrt{2}$ where $a_2, b_2 \in Q$ and are not simultaneously zero.

Now, $$xy^{-1} = (a_1 + b_1\sqrt{2}).\frac{1}{a_2+b_2\sqrt{2}}$$

$$= \frac{a_1+b_1\sqrt{2}}{a_2+b_2\sqrt{2}}.\frac{a_2-b_2\sqrt{2}}{a_2-b_2\sqrt{2}}$$

$$= \frac{a_1a_2-a_1b_2\sqrt{2}+a_2b_1\sqrt{2}-2b_1b_2}{{a_2}^2-2{b_2}^2}$$

$$= \frac{(a_1a_2-2b_1b_2)+(a_2b_1-a_1b_2)\sqrt{2}}{{a_2}^2-2{b_2}^2}$$

$$= \left(\frac{a_1a_2-2b_1b_2}{{a_2}^2-2{b_2}^2}\right) + \left(\frac{a_2b_1-a_1b_2}{{a_2}^2-2{b_2}^2}\right)\sqrt{2}$$

$$= A + B\sqrt{2} \in H$$

Where $A = \left(\frac{a_1a_2-2b_1b_2}{{a_2}^2-2{b_2}^2}\right)$ and $B = \left(\frac{a_2b_1-a_1b_2}{{a_2}^2-2{b_2}^2}\right) \in Q$

Since $x, y \in H \Rightarrow xy^{-1} \in H$

Hence $(H,\bullet)$ is a subgroup of group of group $(R - \{0\},\bullet)$.

Q. No.10

Let H be the set of complex numbers of the form $a + b\sqrt{-5}$, where $a, b \in Q$ and both are not simultaneously zero. Show that H is a subgroup of the group of non-zero complex numbers under multiplication.

Solution

Let $H = \{a + b\sqrt{-5} : a, b \in Q\}$ where a, b are not simultaneously zero.

We are to prove that $(H,\bullet)$ is a subgroup of the group $(C - \{(0,0)\},\bullet)$.

Let $x, y \in H$, Obviously, $H \subseteq C - \{(0,0)\}$

Then $x = a_1 + b_1\sqrt{-5}$ (where $a_1, b_1 \in Q$ and are not simultaneously zero.)

And $y = a_2 + b_2\sqrt{-5}$ (where $a_2, b_2 \in Q$ and are not simultaneously zero.)

Now, $$xy^{-1} = (a_1 + b_1\sqrt{-5}).\frac{1}{a_2+b_2\sqrt{-5}}$$

$$= \frac{a_1+ib_1\sqrt{5}}{a_2+ib_2\sqrt{5}}.\frac{a_2-ib_2\sqrt{5}}{a_2-ib_2\sqrt{5}}$$

$$= \frac{a_1a_2-ia_1b_2\sqrt{5}+ia_2b_1\sqrt{5}-5b_1b_2}{{a_2}^2+5{b_2}^2}$$

$$= \frac{(a_1a_2-5b_1b_2)+i(a_2b_1-a_1b_2)\sqrt{5}}{{a_2}^2+5{b_2}^2}$$

$$= \left(\frac{a_1a_2-5b_1b_2}{a_2^2+5b_2^2}\right) + i\left(\frac{a_2b_1-a_1b_2}{a_2^2+5b_2^2}\right)\sqrt{5}$$

$$= A + iB\sqrt{5} \in H$$

Where $A = \left(\frac{a_1a_2-5b_1b_2}{a_2^2+5b_2^2}\right)$ and $B = \left(\frac{a_2b_1-a_1b_2}{a_2^2+5b_2^2}\right) \in Q$

Since $x, y \in H \Rightarrow xy^{-1} \in H$

Hence $(H,\bullet)$ is a subgroup of group of group $(R-\{(0,0)\},\bullet)$.

Q. No.11

Let $G = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in R,\ ad-bc \neq 0\right\}$ be the group of all 2×2 real matrices under multiplication. Show that the sets

(i) $H = \left\{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a,b,d \in R,\ ad \neq 0\right\}$ **and**

(ii) $K = \left\{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in R\right\}$

are subgroups of G.

Solution

Here $G = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in R,\ ad-bc \neq 0\right\}$ is the group of all 2×2 non-singular real matrices under multiplication.

(i) The set $H = \left\{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a,b,d \in R,\ ad \neq 0\right\}$ is a subset of G.

Now the set H will be the subgroup of group G if

$$A, B \in H \Rightarrow AB^{-1} \in H;\ \forall\ A, B \in H$$

Let $A, B \in H$

Then $A = \begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix}$ where $a_1, b_1, d_1 \in R$ and $a_1d_1 \neq 0$

And $B = \begin{bmatrix} a_2 & b_2 \\ 0 & d_2 \end{bmatrix}$ where $a_2, b_2, d_2 \in R$ and $a_2d_2 \neq 0$ $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

$\text{Adj } A = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

Now $AB^{-1} = A.\frac{1}{|B|}adj(B)$

$$= \begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix}.\frac{1}{a_2d_2}\begin{bmatrix} d_2 & -b_2 \\ 0 & a_2 \end{bmatrix}$$

$$= \frac{1}{a_2d_2}\begin{bmatrix} a_1d_2 & -a_1b_2+a_2b_1 \\ 0 & a_2d_1 \end{bmatrix}$$

$$= \begin{bmatrix} \frac{a_1a_2}{a_2d_2} & \frac{a_2b_1-a_1b_2}{a_2d_2} \\ 0 & \frac{a_2d_1}{a_2d_2} \end{bmatrix}$$

Where $\frac{a_1}{a_2}, \frac{a_2b_1-a_1b_2}{a_2d_2}, \frac{d_1}{d_2} \in R$ $\because a_i, b_i, d_i \in R$ and $a_id_i \neq 0$

Also $\left(\frac{a_1}{a_2}\right)\left(\frac{d_1}{d_2}\right) \neq 0$ $\because a_id_i \neq 0$

Hence $AB^{-1} \in H$

Since $A, B \in H \Rightarrow AB^{-1} \in H$

Therefore H is a subgroup of the group G.

(ii) The set $K = \left\{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in R\right\}$ is a subset of G.

Let $A, B \in K$

Then $A = \begin{bmatrix} 1 & b_1 \\ 0 & 1 \end{bmatrix}$ where $b_1 \in R$ & $B = \begin{bmatrix} 1 & b_2 \\ 0 & 1 \end{bmatrix}$ where $b_2 \in R$

Now $AB^{-1} = A.\frac{1}{|B|}adj(B)$

$$= \begin{bmatrix} 1 & b_1 \\ 0 & 1 \end{bmatrix}.\frac{1}{1}\begin{bmatrix} 1 & -b_2 \\ 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & -b_2 + b_1 \\ 0 & 1 \end{bmatrix} \quad \text{Where } b_1 - b_2 \in R$$

Hence $AB^{-1} \in K$

Since $A, B \in K \Rightarrow AB^{-1} \in K$

Therefore K is a subgroup of the group G.

Q. No.12

Let H and K be two finite subgroup of a group G, whose orders are relatively prime. Prove that $H \cap K = \{e\}$

Solution

Let $O(H) = m$ and $O(K) = n$ Where m and n are relatively prime.

i.e. $G.C.D$ of m, n is 1 Greatest common divisor.

Let $x \in (H \cap K) \Rightarrow x \in H$ and $x \in K$

Let $O(x) = p$ i.e. $x^p = e$

We know that order of an element divides the order group.

$\therefore$ $O(x)$ divides $O(H)$ and $O(x)$ divides $O(K)$

$\Rightarrow$ p divides m and p divides n

$\Rightarrow$ $p = 1$ $\because$ $G.C.D$ of m, n is 1

Hence $x^p = e \Rightarrow x = e$ $(\because p = 1)$

Thus $H \cap K = \{e\}$

Q. No.13

Let $(Z, +)$ be the group of integers. Write two subsets of Z which are closed under addition but are not subgroups of Z.

Solution

$$Z = \{0, \pm 1, \pm 2, \pm 3, \ldots\ldots\}.$$

Let $H = \{1,2,3, \ldots\ldots\}$ and $K = \{-1, -2, -3, \ldots\ldots\}$

Then clearly $H, K \subseteq Z$

Since $\forall\ a, b \in H,\ a + b \in H$ $\therefore$ H is closed over "+"

Similarly $\forall\ a, b \in K,\ a + b \in K$ $\therefore$ K is closed over "+"

But H is not a group $\because$ $\forall\ a \in H,\ a^{-1} \notin H$

Similarly K is not a group $\because$ $\forall\ a \in K,\ a^{-1} \notin K$

e is not in both K, H

Q. No.14

If H is a subgroup of a group G then show that

$$H.H = \{h_1h_2 : h_1, h_2 \in H\} = H$$

Solution

Here H is a subgroup of a group G we have to show that

$$H.H = \{h_1h_2 : h_1, h_2 \in H\} = H$$

For this we have to prove that $H.H \subseteq H$ and $H \subseteq H.H$

Let $h_1h_2 \in H.H \Rightarrow h_1, h_2 \in H$ By definition of $H.H$

$\Rightarrow h_1h_2 \in H$ $\because$ H is a subgroup of G.

Hence $H.H \subseteq H$ ..... (1)

Let $h \in H \Rightarrow h = he \in H.H$

Hence $H \subseteq H.H$ ..... (2)

From (1) and (2) we have

$$H.H = H$$

Q. No.15

Let H and K be subgroup of an abelian group G. Show that the set $HK = \{hk : h \in H, k \in K\}$ is a subgroup of G.

Solution

Let $x, y \in HK$

Then $x = h_1k_1$, $h_1 \in H$, $k_1 \in K$

And $y = h_2k_2$, $h_2 \in H$, $k_2 \in K$

Now $xy^{-1} = (h_1k_1)(h_2k_2)^{-1}$

$= h_1k_1.k_2^{-1}h_2^{-1}$ $\because$ $(ab)^{-1} = b^{-1}a^{-1}$

$= h_1k_1h_2^{-1}k_2^{-1}$ $\because$ G is an abelian group.

$= h_1h_2^{-1}k_1k_2^{-1}$ $\because$ G is an abelian group.

$= (h_1h_2^{-1})(k_1k_2^{-1}) \in HK$

$\because$ $h_1, h_2^{-1} \in H$ $\therefore$ $h_1h_2^{-1} \in H$ $\because$ H is a subgroup of G.

Similarly $k_1, k_2^{-1} \in K$ $\therefore$ $k_1k_2^{-1} \in K$ $\because$ K is a subgroup of G.

Since $\forall\ x, y \in HK \Rightarrow xy^{-1} \in HK$

Therefore HK is a subgroup of G.

Q. No.16

Let H is a subgroup of a group G and $a \in G$ if

$(Ha)^{-1} = \{(ha)^{-1} : h \in H\}$,

Then show that $(Ha)^{-1} = a^{-1}H$

Solution

Here H is a subgroup of a group G we have to show that

$$(Ha)^{-1} = \{(ha)^{-1} : h \in H\} = a^{-1}H$$

For this we have to prove that

$(Ha)^{-1} \subseteq a^{-1}H$ and $a^{-1}H \subseteq (Ha)^{-1}$

Let $x \in (Ha)^{-1} \Rightarrow x = (ha)^{-1}, \quad h \in H$

$= a^{-1}h^{-1} \quad \because (ab)^{-1} = b^{-1}a^{-1}$

$= a^{-1}h^{-1} \in a^{-1}H \quad \because h^{-1} \in H$

Hence $(Ha)^{-1} \subseteq a^{-1}H$ ..... (1)

Let $x \in a^{-1}H \Rightarrow x = a^{-1}h, \quad h \in H$

$= a^{-1}(h^{-1})^{-1} \quad \because (a^{-1})^{-1} = a$

$= (h^{-1}a)^{-1} \quad \because b^{-1}a^{-1} = (ab)^{-1}$

$= (h^{-1}a)^{-1} \in (Ha)^{-1} \quad \because h^{-1} \in H$

Hence $a^{-1}H \subseteq (Ha)^{-1}$ ..... (2)

From (1) and (2) we have

$(Ha)^{-1} = a^{-1}H$

Q. No.17

Let H and K be two finite subgroup of a group G and $g \in G$.

Prove that $g(H \cap K) = gH \cap gK$

Solution

Let H and K be two finite subgroup of a group G and $g \in G$.

We have to prove that $g(H \cap K) = gH \cap gK$

For this we have to prove that

$g(H \cap K) \subseteq gH \cap gK$ and $gH \cap gK \subseteq g(H \cap K)$

Let $x \in g(H \cap K) \Rightarrow g^{-1}x \in (H \cap K)$

$\Rightarrow g^{-1}x \in H$ and $g^{-1}x \in K$

$\Rightarrow x \in gH$ and $x \in gK$

$\Rightarrow x \in gH \cap gK$

Hence $g(H \cap K) \subseteq gH \cap gK$ ..... (1)

Let $x \in gH \cap gK \Rightarrow x \in gH$ and $x \in gK$

$\Rightarrow g^{-1}x \in H$ and $g^{-1}x \in K$

$\Rightarrow g^{-1}x \in (H \cap K)$

$\Rightarrow x \in g(H \cap K)$

Hence $gH \cap gK \subseteq g(H \cap K)$ ..... (2)

From (1) and (2) we have

$g(H \cap K) = gH \cap gK$

Q. No.18

Which of the following subsets of the group $(\bar{Z}_{13}, \bullet)$ of the non-zero residue classes under multiplication modulo 13 are subgroup of $\bar{Z}_{13}$.

$H_1 = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}, \bar{9}, \overline{11}\}$, $H_2 = \{\bar{1}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}, \overline{12}\}$,

$H_3 = \{\bar{1}, \bar{6}, \bar{8}, \overline{10}\}$, $H_4 = \{\bar{1}, \bar{3}, \bar{9}\}$.

Solution

Here $\bar{Z}_{13} = \{\bar{1}, \bar{2}, \bar{3}, \ldots\ldots, \overline{12}\}$ is group under multiplication modulo 13 and

$H_1 = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}, \bar{9}, \overline{11}\}$ $H_2 = \{\bar{1}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}, \overline{12}\}$,

$H_3 = \{\bar{1}, \bar{6}, \bar{8}, \overline{10}\}$, $H_4 = \{\bar{1}, \bar{3}, \bar{9}\}$

are subsets of $\bar{Z}_{13}$.

Now, $H_1 = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}, \bar{9}, \overline{11}\}$ is not a subgroup of $\bar{Z}_{13}$.

$\because \quad \bar{3}.\bar{7} = \bar{8} \notin H_1$

$H_2 = \{\bar{1}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}, \overline{12}\}$ is not a subgroup of $\bar{Z}_{13}$.

$\because \quad \bar{2}.\bar{8} = \bar{3} \notin H_2$

$H_3 = \{\bar{1}, \bar{6}, \bar{8}, \overline{10}\}$ is not a subgroup of $\bar{Z}_{13}$.

$\because \quad \bar{6}.\bar{8} = \bar{9} \notin H_3$

Here, $H_4 = \{\bar{1}, \bar{3}, \bar{9}\}$

$\bullet$	$\bar{1}$	$\bar{3}$	$\bar{9}$
$\bar{1}$	$\bar{1}$	$\bar{3}$	$\bar{9}$
$\bar{3}$	$\bar{3}$	$\bar{9}$	$\bar{1}$
$\bar{9}$	$\bar{9}$	$\bar{1}$	$\bar{3}$

Let $\bar{a}, \bar{b} \in H_4$ then $\bar{a} \bullet \bar{b} = \bar{r}$, where $\bar{r}$ is the remainder obtained after the division of $\bar{a} \bullet \bar{b}$ by 13 when $\bar{a} \bullet \bar{b}$ equals or exceed 13.

e.g. $\bar{3} \bullet \bar{1} = \bar{3}$ & $\bar{3} \bullet \bar{9} = \bar{1}$

(I) Multiplication modulo 13 is closed over H_4

i.e $\bar{a} \bullet \bar{b} \in H_4$; $\forall\, a, b \in H_4$

(It is clear from the table.)

(II) Multiplication modulo 13 is associative over H_4.

i.e. $(\bar{a} \bullet \bar{b}) \bullet \bar{c} = \bar{a} \bullet (\bar{b} \bullet \bar{c})$; $\forall\, a, b, c \in H_4$

Take $\bar{1}, \bar{3}, \bar{9} \in H_4$

$(\bar{1} \bullet \bar{3}) \bullet \bar{9} = \bar{3} \bullet \bar{9}$ $\quad$ $\bar{1} \bullet (\bar{3} \bullet \bar{9}) = \bar{1} \bullet \bar{1}$

$= \bar{1}$ $\quad$ $= \bar{1}$

Clearly $(\bar{1} \bullet \bar{3}) \bullet \bar{9} = \bar{1} \bullet (\bar{3} \bullet \bar{9})$

(III) $\bar{1}$ is an identity element of H_4.

$\because \quad \bar{1} \bullet \bar{a} = \bar{a} \bullet \bar{1} = \bar{a}$; $\forall\, \bar{a} \in H_4$ (It is clear from the table.)

(IV) $(\bar{1})^{-1} = \bar{1}$, $(\bar{3})^{-1} = \bar{9}$, $(\bar{9})^{-1} = \bar{3}$ (It is clear from the table.)

Thus H_4 is a subgroup of $\bar{Z}_{13}$ under the multiplication modulo 13.