

Prove that every subgroup of a cyclic group is cyclic.

Let $G = \langle a \rangle$ be a cyclic group generated by a .

Let H be a Subgroup of G .

To prove H is cyclic

If $H = \{e\}$ or $H = G$, then clearly H is cyclic

If $H \neq \{e\}$ and $H \neq G$

Since, H is subgroup of G and G is cyclic hence each element of H is some integral power of a .

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

Let $S > m$, such that $a^S \in H$

Thus we can write -

$S = mq + r$, where q is (+ve) integer and $0 \leq r < m$

$$\therefore S - mq = r \quad \text{--- (1)}$$

Now, $a^S \in H$, $a^m \in H$

$$\Rightarrow a^S \in H, (a^m)^q \in H$$

$$\Rightarrow a^S \in H, a^{mq} \in H$$

$$\Rightarrow a^S \in H, a^{-mq} \in H$$

$$\Rightarrow a^S a^{-mq} \in H \quad (\text{by closure property})$$

$$= a^{S-mq} \in H$$

$$= a^r \in H \quad \text{by (1)}$$

\because any integral power of group element is also a group element

$\because H$ is sub-group so its elements are invertible

Since, $r < m$ and m is the least (+ve) integer such that $a^m \in H$.
So above is possible only when $r = 0$

where $r = 0$

$$\therefore S = mq$$

$$\therefore a^S = a^{mq} = (a^m)^q$$

Since, a^S is arbitrary element of H and it is some integral power of a^m .
 $\therefore H$ is cyclic generated by a^m .

powers of a^m , hence we can say H is cyclic generated by a^m . Hence every sub-group of a cyclic group is cyclic.

Theorem 2 If H is a subgroup of a group G then prove that $H^{-1} = H$.
Is converse true?

Proof - Let h be an arbitrary element of H

Then $h \in H \Rightarrow h^{-1} \in H$

$\Rightarrow (h^{-1})^{-1} \in H$ ~~$\Rightarrow h \in H$~~

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

$\therefore H \subseteq H^{-1}$ — (1)

Note:
 $H = \{h, m, n, \dots\}$
 $H^{-1} = \{h^{-1}, m^{-1}, n^{-1}, \dots\}$

again,

let $h^{-1} \in H^{-1} \Rightarrow h \in H \Rightarrow h^{-1} \in H$ $\{ \therefore H \text{ is subgroup} \}$

So $H^{-1} \subseteq H$ — (2)

from (1) and (2), $H = H^{-1}$

~~Proof~~ Converse is not true, which is below:-

$G = \{1, -1\}$, $H = \{-1\}$. $\therefore (-1)^{-1} = -1$ but $-1 \in H$, $1 \in H \Rightarrow 1 \in H$ [Cyclic]
But $1 \notin H$

Corollary - The necessary and sufficient condition for a complex H of a group G to be a sub-group is that $HH^{-1} = H$

Theorem 3 If H and K are subgroups of a group G then prove that HK is a subgroup of G iff $HK = KH$ (or H and K are commute)

Ans - Let HK be the subgroup of the group G .

To prove $HK = KH$

Since H, K, HK are sub groups.

$\therefore H = H^{-1}$, $K = K^{-1}$ and $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$
[$K^{-1} = K$, $H = H^{-1}$]

Converse \rightarrow Let $HK = KH$

To prove HK is subgroup, it is sufficient to prove that -

$$(HK)(HK)^{-1} = HK \quad \{\because HH^{-1} = H\}$$

Now,

$$\begin{aligned} (HK)(HK)^{-1} &= (HK)(K^{-1}H^{-1}) \\ &= H\{(KK^{-1})H^{-1}\} \quad (\text{By ass. law}) \\ &= H(KH^{-1}) \quad \{K \text{ is subgroup?}\} \\ &= (HK)H^{-1} \quad [\text{By ass. Law}] \\ &= (KH)H^{-1} \quad [\because HK = KH] \end{aligned}$$

$$\begin{aligned} (HK)(HK)^{-1} &= K(HH^{-1}) \\ &= KH \quad [\because H \text{ is subgroup } \therefore HH^{-1} = H] \\ &= HK \quad [\because HK = KH] \end{aligned}$$

$\Rightarrow HK$ is a subgroup of G

Note - If a group of order prime, then it must be cyclic.

Theorem (9) \times The union of two subgroups of a group G iff one contains the other.

Ans Let H_1 and H_2 be subgroup of a group G

Let $H_1 \subset H_2$ or $H_2 \subset H_1$

To prove that, $H_1 \cup H_2$ is a subgroup of G

$$H_1 \subset H_2 \Rightarrow H_1 \cup H_2 = H_2$$

Also H_2 is a subgroup of G

$\Rightarrow H_1 \cup H_2$ is a subgroup of G

again,

$$H_2 \subset H_1 \Rightarrow H_1 \cup H_2 = H_1$$

Also H_1 is a subgroup of G

$\Rightarrow H_1 \cup H_2$ is a subgroup of G

Conversely:-

Suppose that H_1 and H_2 are subgroups of a group G such that $H_1 \cup H_2$ is a sub-group of G

To prove that-

$$H_1 \subset H_2 \text{ or } H_2 \subset H_1$$

Suppose the contrary. Then $H_1 \not\subset H_2$ or $H_2 \not\subset H_1$

$$H_1 \not\subset H_2 \Rightarrow \exists a \in H_1 \text{ such that } a \notin H_2$$

$$H_2 \not\subset H_1 \Rightarrow \exists b \in H_2 \text{ such that } b \notin H_1$$

Also $H_1 \cup H_2$ is a subgroup of G

$$\therefore ab \in H_1 \cup H_2$$

This $\Rightarrow ab \in H_1$ or $ab \in H_2$

$$a \in H_1, ab \in H_1 \Rightarrow a^{-1}(ab) \in H_1$$

Since H_1 is a sub-group

$$\Rightarrow (a^{-1}a)b \in H_1 \Rightarrow b = eb \in H_1 \Rightarrow b \in H_1$$

A contradiction for $b \in H_1$

$b \in H_2, ab \in H_2 \Rightarrow (ab)b^{-1} \in H_2$ for H_2 is a sub-group

$$\Rightarrow a \in H_2$$

$$\text{for } (ab)b^{-1} = a(bb^{-1}) = ae = a$$

again, we get a contradiction for $a \notin H_2$

\therefore In either initial assumption is wrong
consequently $H_1 \subset H_2$ or $H_2 \subset H_1$

Right coset - Let H be a sub group of a group G

Let $a \in G$ then the set

$$Ha = \{ha : h \in H\}$$

$$\left\{ \begin{array}{l} \{h_1, h_2, h_3, \dots\} \\ Ha = \{ah_1, ah_2, ah_3, \dots\} \end{array} \right.$$

is called the right coset of H in G with respect to a

* $G = \{1, 2, 3, 4, 5, 6\}$ { mod 6 } multiplication on subgroup

$$H = \{1, 2, 4\}, H \cdot 1 = H, H \cdot 2 = H, H \cdot 4 = H$$

$$H \cdot 3 = \{3, 6, 5\}$$

$$\therefore G = \{H, H \cdot 3\}$$

$$H \cdot 5 = H \cdot 6 = H \cdot 3$$

Left coset - Let H be a subgroup of a group G .

Let $a \in G$, then the set

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

is called the left coset of H in G w.r.t. " a ".

Remark - If h be any element of subgroup H of a group G then

$$hH = H \text{ and } Hh = H$$

→ [This theorem see on page - (68), 2014]

Theorem ⑤

Prove that $aH = bH$ (iff) $a^{-1}b \in H$ [If a, b be two elements of a group G and H be a subgroup of G then $a^{-1}b \in H$ if and only if $aH = bH$]

Ans First we shall suppose that $aH = bH$ and ^{to} prove ~~that~~ $a^{-1}b \in H$

$$\therefore aH = bH$$

$$\therefore a^{-1}aH = a^{-1}bH$$

$$\therefore eH = a^{-1}bH$$

$$\therefore H = a^{-1}bH$$

$$\therefore a^{-1}b \in H \quad [\because H = bH \Rightarrow b \in H]$$

Now, we shall suppose that $a^{-1}b \in H$ and prove that

$$aH = bH$$

$$\therefore a^{-1}b \in H$$

$$\therefore a^{-1}bH = H$$

$$\Rightarrow a(a^{-1}b)H = aH$$

$$\Rightarrow (aa^{-1})bH = aH$$

$$\Rightarrow e bH = aH$$

$$\Rightarrow bH = aH \quad \text{Proved}$$

Remark Similarly for $Ha = Hb \Rightarrow ba^{-1} \in H$

Thm. 1.1 Prove that any two left cosets of a subgroup in a group are either disjoint or identical

Ans: Let H be a sub-group of a group G

Let aH and bH be any two left co-sets of H , ~~in G~~

where $a, b \in G$

We shall prove that $aH = bH$ or $aH \cap bH = \emptyset$

Where \emptyset denotes the null set

We suppose that $aH \cap bH \neq \emptyset$ then there exist at least one common element of aH and bH .

Let $ah_1 = bh_2$, where $h_1, h_2 \in H$ and $a, b \in G$

Let e be the identity element of H or G

$$\text{Now, } ah_1 = bh_2$$

$$\Rightarrow ah_1h_1^{-1} = bh_2h_1^{-1}$$

$$\Rightarrow ae = bh_2h_1^{-1}$$

$$\Rightarrow a = bh_2h_1^{-1}$$

$$\Rightarrow aH = bh_2 h_1^{-1} H \text{ --- ①}$$

Since $h_2 \in H, h_1 \in H$, so $h_1^{-1} \in H$

$\therefore h_2 h_1^{-1} \in H$ [By closure property]

$$\therefore h_2 h_1^{-1} H = H \text{ --- ② [} \cancel{H} H = H \Rightarrow h \in N \text{]}$$

from ① and ② we have

$$ah_1 = bh_2 \Rightarrow aH = bH$$

Hence aH and bH are either disjoint or identical.

Remark → Similarly we can prove that any two right cosets are either disjoint or identical.