

COSETS

COSETS

If H is a subgroup of G , the set aH is called the left coset of H in G containing a , where aH is called the right coset of H in G containing a .

The element " a " is called the representative of aH (or Ha) of the group operation is $+$, then the right and left cosets of H in G represented by the element $a \in G$ are

$H+a = \{h+a \mid h \in H\}$ and $a+H = \{a+h \mid h \in H\}$ respectively.

The number of elements in aH (or Ha) is denoted by $|aH|$ (or $|Ha|$)

Example:-

Let $H = \{0, \pm 3, \pm 6, \dots\}$. Find all left cosets of H in $\mathbb{Z}$.

Solution:- The left cosets of H in $\mathbb{Z}$ are

$$0+H = H,$$

$$1+H = \{\dots, -5, -2, 1, 4, 7, \dots\}$$

$$2+H = \{\dots, -4, -1, 2, 5, 8, \dots\}$$

$$3+H = \{\dots, -3, 0, 3, 6, 9, \dots\} = 0+H = H$$

$$4+H = 1+H$$

$$5+H = 2+H \text{ and so on.}$$

Thus, the distinct cosets are $H, 1+H$ and $2+H$.

Example:-

Let n be an integer greater than 1. Let $H = \{0, \pm n, \pm 2n, \pm 3n, \dots\}$ find all left coset of H in $\mathbb{Z}$. How many are there?

Solution:-

The left coset of H are $H, 1+H$ and $2+H, \dots, H+(n-1)$

The number of left coset is n .

PROPERTIES OF COSETS:-

Let H be a subgroup of G and let $a, b \in G$. Then

(a) $a \in aH$ [or equivalently $a \in Ha$]

(b) $aH = H \Leftrightarrow a \in H$ [or equivalently $Ha = H \Leftrightarrow a \in H$]

(c) $aH = bH$ or $aH \cap bH = \emptyset$

(d) $aH = bH \Rightarrow a^{-1}bH = \emptyset$

(e) $|aH| = |bH|$

(f) $aH = Ha \Leftrightarrow H = aHa^{-1}$

(g) aH is a subgroup of G if and only if $a \in H$.

Proof:-

(a) Let $a \in G$

then $a = ae$, where e is the identity element of G .

But $e \in H$
Therefore, $a \in aH$
[Or equivalently $a = ea$ and $e \in H \Rightarrow a \in aH$]

(b) Firstly, let us assume that $aH = H$

Then $a = ae \in aH = H$

Conversely, let us assume that $a \in H$

We will show that $aH \subseteq H$ and $H \subseteq aH$.

Now any element of aH is of the form ah , where $h \in H$
 $ah \in H$, since $h \in H$ and $a \in H$.

Thus $aH \subseteq H$

To show that $aH \subseteq H$

Let $h \in H$

Since $a \in H$ and $h \in H$, therefore $a^{-1}h \in H$

Thus, $h = eh = (aa^{-1})h = a(a^{-1}h) \in aH$

$\therefore H \subseteq aH$

Hence $aH \subseteq H$ and $H \subseteq aH$

$\Rightarrow aH = H$.

(c) Suppose $aH \cap bH \neq \emptyset$.

Then prove that $aH = bH$

Let $x \in aH \cap bH$

Then $\exists h_1, h_2 \in H$ such as $x = ah_1$ and $x = bh_2$

Thus, $ah = (ah_1^{-1})h = a(ch_1^{-1}h) = (bh_2)(ch_1^{-1}h) = bh_3$, where $h_3 = hah_1^{-1}h_2$

Thus, $a(bH) = b(b_3H)$

$\Rightarrow aH = bH$ [$\because b_3H = H$ by (b)]

(d) $aH = bH$

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

$\Leftrightarrow a^{-1}b \in H$ [by (b) i.e. $aH = H \Leftrightarrow a \in H$]

otherwise

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

$\Rightarrow a^{-1}bH = He = H$

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

conversely

$ab^{-1} \in H$

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

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

$\Rightarrow bH = aH$

(e) Define a function $\varphi: aH \rightarrow bH$ by $\varphi(ah) = bh \ \forall h \in H$

To show that φ is one-to-one and on to.

Suppose $\varphi(ah_1) = \varphi(ah_2)$, $h_1, h_2 \in H$.

$$\Rightarrow bh_1 = bh_2 \text{ [definition of } \varphi]$$

$$\Rightarrow h_1 = h_2 \text{ [cancellation law]}$$

$$\Rightarrow ah_1 = ah_2 \text{ i.e. } \varphi \text{ is one-to-one.}$$

St $bh_1 \neq bh_2$, then $h_1 \neq h_2$

St shows that only two identical elements of aH can have identical images and two unequal images, can't have the same pre-image.

For φ on to, we have to show that for every $x \in bH$, there exist at least one y in aH such that $x = \varphi(y)$.

Thus every element of aH corresponds to only one element of bH and vice versa.

Thus the elements of aH and bH are in one-to-one correspondence

Let $bh' \in bH$

$$\Rightarrow h' \in H$$

$$\Rightarrow ah' \in aH$$

By definition of φ , $\varphi(ah') = bh'$

Thus corresponding to any element $x = bh' \in bH$, there exists an element ah' in aH . Hence all elements of bH are covered by the function φ and no element of bH are left out.

Hence φ is on to.

So, φ defines as one-to-one, on to function from aH to bH .

(f) we have $aH = Ha$

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

$$\Rightarrow aHa^{-1} = Ha^{-1}a = H$$

(g) Suppose aH is a subgroup of G

Then $e \in aH$, e being the identity.

Thus $aH \cap eH \neq \emptyset$

By (c), we have $aH = eH = H$

By (b), we have $a \in H$

conversely, let $a \in H$

Again by (b) $aH = H$

LAGRANGES THEOREM:-

St H is a subgroup of the finite group G then $|aH|$ is a divisor of $|G|$ i.e., $|aH| \mid |G|$.

Proof: -

Since G is a finite group then $o(G)$ is finite. As H is the subgroup of G , so $o(H)$ is also finite.

Let $o(H) = n$. So H contains 'n' distinct elements.

Let $H = \{h_1, h_2, h_3, \dots, h_n\}$ where $h_i \neq h_j \forall i \neq j$.

Now if $H = G \Rightarrow o(H) = o(G)$

So $o(H) | o(G)$ and hence the theorem.

If $H \neq G$, then $\exists$ at least one element $a \in G$ & $a \notin H$.

Let us construct a left coset aH of H and denote it by H_1 .

$\therefore H_1 = aH = \{ah_1, ah_2, \dots, ah_n\}$

Now if possible let $ah_i = ah_j \Rightarrow h_i = h_j$ which is contradiction.

Hence the element of H_1 are distinct.

Now we have to show, $H \cap H_1 = \emptyset$

If possible let $h_1 \in H$ and $ah_k \in aH$.

Such that $h_1 = ah_k \Rightarrow h_1 h_k^{-1} = a$

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

$\therefore h_1 h_k^{-1} \in H \Rightarrow a \in H$ which is a contradiction.

$\therefore H \cap H_1 = \emptyset$

If $H \cup H_1 = G$

$\Rightarrow o(H \cup H_1) = o(G)$

$\Rightarrow 2o(H) = o(G)$

$\Rightarrow o(H) | o(G)$ and hence the theorem.

If $H \cup H_1 \neq G$ then continuing in this manner and G is finite then we will have finite number of cosets (say m cosets) of H $\exists H \cup H_1 \cup H_2 \cup \dots \cup H_m = G$

$\Rightarrow o(H \cup H_1 \cup H_2 \cup \dots \cup H_m) = o(G)$

$\Rightarrow (m+1)o(H) = o(G)$

$\Rightarrow o(H) | o(G)$

So $o(H)$ is a divisor of $o(G)$ and hence the theorem.

INDEX OF THE SUBGROUP:-

If H is a subgroup of a group G then the number of distinct right or left cosets of H in G is called the index of H in G and is denoted by

$$i_{GH} = \frac{o(G)}{o(H)} \text{ or } |G:H| = \frac{|G|}{|H|}$$

Corollary:-

If G is the finite group and $a \in G$ then $o(a) | o(G)$

Proof:-

Let us construct the cyclic group H , where 'a' is the generator.

$\therefore H = \{a^x \mid a \in G \text{ and } x \text{ is any integer}\}$

Let the order of the generator a is n . So by definition $a^n = e \dots (1)$

Now our aim to show H contains exactly n elements

Let m is any integer $\ni m > n$ and $a^m \in H$.

Since $m > n$, then by division algorithm $\exists$ integers k and $r \ni m = nk + r$ where $0 \leq r < n$

$$\therefore a^m = a^{nk+r} = a^{nk} \cdot a^r = (a^n)^k \cdot a^r = e^k \cdot a^r = a^r \quad (\text{using (1)})$$

$$\therefore a^m = a^r$$

If $m > n$ then a^m is any one of the elements $a, a^2, a^3, \dots, a^n$.

So H cannot contain more than n elements.

Now to establish that it contains exactly n elements it will sufficient if we can show that there are no two elements of H are same.

It possible let $a^m = a^k$ where $0 < k < m$

$\Rightarrow a^{m-k} = e$ where $m-k$ is a positive integer less than n .

This result is not possible since n is the order of a . So $a^{m-k} \neq e$ and this shows $a^m \neq a^k$. So the elements of H are distinct and H contains exactly n elements.

Hence the order of the cyclic group H is same as its generator a .

$$\therefore o(H) = o(a)$$

By Lagrange's theorem, we know $o(H) | o(G) \Rightarrow o(a) | o(G)$

Corollary:-2

If G is the finite group and $a \in G$ then $a^{o(G)} = e$

Proof:-

We know $o(a) | o(G)$

$\Rightarrow \exists$ a +ve integer $k \ni o(G) = k \cdot o(a)$

$$\therefore a^{o(G)} = a^{k \cdot o(a)} = [a^{o(a)}]^k = e^k = e$$

$$\therefore a^{o(G)} = e$$

Corollary:-3

If G is a finite group whose order is a prime number p , then G is a cyclic group.

Proof:-

Given $o(G) = p$ which is a prime number.

Let $a \in G$ is any element $\ni$ its order is n .

So by definition of order of an element, $a^n = e$.

Now, let us construct a cyclic subgroup generated by ' a '.

$$\therefore H = \{a, a^2, a^3, \dots, a^n = e\}$$

Let m is any integer $\ni m > n$ and $a^m \in H$

Since $m > n$ then by division algorithm $\exists$ integers k and $r \ni m = nk + r$ where

$$0 \leq r < n$$

$$\therefore a^m = a^{nk+r} = a^{nk} \cdot a^r$$

$$= (a^n)^k \cdot a^r = e^k \cdot a^r = e \cdot a^r = a^r$$

gt $m > n$ then a^m is any one of the elements $a, a^2, a^3, \dots, a^n$.

So H does not contain more than n elements.

Now we will show that H contains exactly n elements.

Let $a^m = a^k$ where $0 < k < m$

$\Rightarrow a^{m-k} = e$, where $n > m-k > 0$ which is contradiction.

Since n is the order of ' a ' and $m-k < n$

Hence H contains exactly n elements i.e., $o(H) = n$

By Lagrange's theorem

$$o(H) \mid o(G) \Rightarrow n \mid p$$

Since p is a prime number and $n \mid p$, then it is possible only when $n = p$.

$$\therefore o(H) = o(G)$$

Since H is the cyclic group then G is the cyclic group.

FERMAT'S THEOREM:-

gt p is a prime number and ' a ' is any integer, then $a^p \equiv a \pmod{p}$.

Proof:- case-I

gt $p \mid a$ then $p \mid (a^{p-1} - 1)$

$$\Rightarrow p \mid (a^p - a)$$

$$\Rightarrow a^p \equiv a \pmod{p}$$

Case-II

gt $p \nmid a$ i.e., $(p, a) = 1$

$\therefore$ By Euler's theorem, we have $a^{\phi(p)} \equiv 1 \pmod{p}$

$$\Rightarrow a^{p-1} \equiv 1 \pmod{p} \quad (\because p \text{ is a prime number } \therefore \phi(p) = p-1)$$

$$\Rightarrow p \mid (a^{p-1} - 1)$$

$$\Rightarrow p \mid (a^p - a)$$

$$\Rightarrow p \mid (a^p - a)$$

$$\Rightarrow a^p \equiv a \pmod{p}$$

Hence Fermat's theorem is proved.

DEFINITION:-

Let H be a subgroup of G . we define a relation ' $\sim$ ' on G by $a \sim b$ iff $aH = bH$ [i.e. $a \sim b$ iff $a^{-1}b \in H$]

Theorem:-

Let H be a subgroup of G . Then the relation ' $\sim$ ' defined by ' $a \sim b$ and only if $a^{-1}b \in H$ ' is an equivalence relation. The equivalence classes are the left cosets of H .

of H in G .

Proof:-

We need to prove that $\sim$ is reflexive, symmetric and transitive.

Reflexive:-

For any $a \in G$, $a^{-1}a = e \in H$

$\therefore a \sim a$ i.e., $\sim$ is reflexive

Symmetric:-

Let $a \sim b$, for any $a, b \in G$, $a^{-1}b \in H$

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

Thus $b \sim a$ i.e., $\sim$ is symmetric.

Transitive:-

Let $a, b, c \in G$; such that $a \sim b$ and $b \sim c$, then $a^{-1}b \in H$ and $b^{-1}c \in H$

$$\begin{aligned}\therefore (a^{-1}b)(b^{-1}c) &= a^{-1}(bb^{-1})c \\ &= a^{-1}c \in H\end{aligned}$$

$\therefore a \sim c$

i.e., $\sim$ is transitive.

Thus $\sim$ is an equivalence relation.

The equivalence class determined by $a \in G$ is

$$\begin{aligned}[a] &= \{b \in G : b \sim a\} \\ &= \{b \in G : b^{-1}a \in H\}\end{aligned}$$

Now we will show that $[a] = aH$

Let $b \in [a]$

Then $bH = aH$

Since $b \in bH$, therefore $b \in aH$

$$[a] \subseteq aH$$

Again consider any element ah to aH

$$\text{Then } (ah)^{-1}a = (h^{-1}a^{-1})a = h^{-1} \in H$$

$\therefore ah \sim a$ i.e., $ah \in [a]$.

This is true for any $ah \in aH$

therefore, $aH \subseteq [a]$,

Thus, we have shown that $[a] = aH$

THEOREM:-

Let H be a subgroup of G . Then there is a one-to-one correspondence between the elements of H and those of any right or left cosets of H .

Proof:-

Let Ha be a right coset of H in G .

(OT)

Alpha Biswas team

consider the function $\varphi: H \rightarrow Ha$, defined by $\varphi(h) = ha$, $h \in H$.

Now for $h_1, h_2 \in H$, $h_1a = h_2a$

$\Rightarrow h_1 = h_2$, by cancellation law.

Therefore φ is one-to-one.

φ is clearly surjective.

Hence there is a one-to-one correspondence between the elements of H and those of Ha .

Similarly the function $\varphi: H \rightarrow aH$ defined by $\varphi(h) = ah$ is bijective.

Thus the elements of H and aH are in one-to-one correspondence.

Note:-

If H is a finite subgroup of a group G , then the number of elements of every coset of H is the same as the number of elements of H .

Now using the above fact, we will prove an elementary theorem about the number of cosets of a subgroup of a finite group.

Example:-

Find the order of H , if H is a proper subgroup of a group of order 68 & H is non-cyclic.

Solution:-

By Lagrange's theorem, $|H|$ divides $|G| = 68$.

Since H is not cyclic and groups of prime order are cyclic, therefore $|H|$ is prime.

Further $|H| \neq 1$, since groups of order 1 contains just the identity and are cyclic.

So, we will find a divisor of 68 which is the prime factorisation.

We have $68 = 2^2 \cdot 17$, which is the prime factorisation.

So $|H| = 4$ or 68

Since H is a proper subgroup, therefore $H \neq G$

So $|H| \neq 68$. Hence $|H| = 4$.

Example:-

Find order of H if H is subgroup of some group of order 100 and H contains no element of order 2, with H non-cyclic.

Solution:-

By Lagrange's theorem, $|H|$ divides $|G| = 100$.

Since H is non-cyclic, therefore, $|H| \neq 1$, $|H| \neq 2$, $|H| \neq 5$.

Hence the possibilities for $|H|$ are 4, 10, 20, 25, 50 and 100.

Now, groups of even order must contain an element of order 2.

Since H does not, it must have odd order.

Thus $|H| = 25$.

Example:-

Let G be a group with subgroups H and K . If $|G| = 660$, $|K| = 66$ and $K \subset H \subset G$, what are the possible values for $|H|$?

Solution:-

By Lagrange's theorem, $|K| = 66$ ($2 \cdot 3 \cdot 11$) divides $|H|$ and $|H|$ divides $|G| = 660 = (2^3 \cdot 3 \cdot 5 \cdot 11)$

Since $K \neq H$, $H \neq G$, therefore $|H| = 2 \cdot (2 \cdot 3 \cdot 11) = 132$ or $5 \cdot (2 \cdot 3 \cdot 11) = 330$

Example:-

If p is prime and $|G| = 2p$, prove that every proper subgroup of G is cyclic. Also prove that if $|G| = p^2$, then G has a subgroup of order p

Solution:-

If H is a proper subgroup of G , then by Lagrange's Theorem, $|H| = 2$ or p

If $|H| = 2$, then $H = \{e, a\}$, where $a^2 = e$

so $|H| = \langle a \rangle$.

If $|H| = p$, let $b \in H$, $b \neq e$

then $|b| = p$.

so, $|H| = \langle b \rangle$.

Further, Let $x \in G$ and $x \neq e$.

then $|x| = p$ or $|x| = p^2$.

If $|x| = p$ then $|\langle x \rangle| = p$.

If $|x| = p^2$, then $G = \langle x \rangle$ and $\langle x \rangle$ is a subgroup of G of order p .

Example:-

Show that every Group G with $|G| < 6$, is abelian.

Solution:- Claim - 1

Let H be a subgroup of G .

then $|H|$ divides $|G|$, (1)

which follows from Lagrange's Theorem.

Claim - 2

If $|G|$ is prime, then G must be cyclic

For any $g \in G$ with $g \neq e$

$H = \langle a \rangle \cong G$

Since $|G|$ is prime and $|H| \geq 1$, therefore by (1), $|H| = |G|$

so $G = H$ is cyclic.

Example:-

Prove that if G is a group of order p^2 and G is not cyclic, then $a^2 = e$ for $\forall a \in G$.

Solution:-

If order of G is p^2 , then the possible orders for the subgroup of G are 1, p or p^2 . (By Lagrange's theorem)

But it is known that there can not be any element of order p because, then that element would generate the group G and by hypothesis, we know that G is not cyclic.

[If $|G| = p^2$, then $e, a, a^2, \dots, a^{p^2-1}$ are all distinct and $\langle a \rangle = \{e, a, a^2, \dots, a^{p^2-1}\} = G$, because $|G| = p^2$]

If $a \in G$, then $\langle a \rangle$ is a subgroup of G .

Therefore, the possible orders for $\langle a \rangle$ could be 1 and p .

If $|\langle a \rangle| = |G| = 1$, then $a^1 = e$

$$\Rightarrow a^p = e$$

If $|\langle a \rangle| = |G| = p$, then $a^p = e$

Example:-

If $G = \langle a \rangle$ and $|G| = 20$. Given $k \mid 20$ and $H = \langle a^k \rangle$. Find $|G:H|$

Solution:-

Since $k \mid 20$, $\exists t \in \mathbb{N}$ such that $20 = kt$

Then $H = \langle a^k \rangle = \{e, a^k, a^{2k}, \dots, a^{(t-1)k}\}$ has t elements.

By Lagrange's Theorem, we have

$$|G:H| = \frac{|G|}{|H|} = \frac{20}{t} = k.$$

Example:-

Given an example of a group G , a subgroup H of G and element $a \in G$, with $|G:H| = 3$ and $a^3 \notin H$.

Solution:-

Take $G = S_3$

$H = \langle (12) \rangle$, $a = (23)$

Then $a \in S_3$,

By Lagrange's theorem, we have $|G:H| = \frac{|G|}{|H|}$

Since $|G| = |S_3| = 6$ and (12) has order 2 i.e. $|H| = 2$, therefore $|G:H| = \frac{6}{2} = 3$

but $a^3 = a \notin H$

Example:-

If G is finite and H is a subgroup of G , prove that $|G:H| = \frac{|G|}{|H|}$

Solution:-

By Lagrange's theorem, $|G| = n|H|$

Since n is the number of left cosets of H in G , i.e. $n = |G:H|$, we have,

$$|G| = |H| |G:H| \Rightarrow |G:H| = \frac{|G|}{|H|}$$

Example:-

Let H and K be subgroups of a finite group G with $K \subseteq H \subseteq G$. Prove that $|G:K| = |G:H| |H:K|$

Solution:-

K is a subgroup of H . Since G is finite, the index of H in G , index of H in G , index of K in G and the index of K in H are all finite.

Hence, by definition of index and Lagrange's Theorem, we get

$$|G:K| = \frac{|G|}{|K|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = |G:H| |H:K|$$

Example:-

Let $G = \mathbb{Z}$, $H = 3\mathbb{Z}$, $K = 15\mathbb{Z}$; verify that $|G:K| = |G:H| |H:K|$

Solution:- To find index of H in G , index of K in H , the index of K in G . Here $K \subseteq H \subseteq G$.

Index of $3\mathbb{Z}$ in $\mathbb{Z}$:-

By definition, $3\mathbb{Z} = \{0, \pm 3, \pm 6, \dots\}$

Now for any integer $m \in \mathbb{Z}$, $m = 3q + r$, $0 \leq r \leq 2$, by division algorithm

$$\text{Here, } 3\mathbb{Z} + m = 3\mathbb{Z} + (3q + r)$$

$$= 3(\mathbb{Z} + q) + r$$

$$= 3\mathbb{Z} + r, \quad 0 \leq r \leq 2 \quad \text{as } 3q \in \mathbb{Z}$$

Thus, we can have at most 3 left cosets of H in G i.e. $H, H+1, H+2$, i.e.,

$$3\mathbb{Z}, 3\mathbb{Z}+1, 3\mathbb{Z}+2.$$

These cosets are distinct

$$\text{i.e. } |G:H| = 3$$

$$\Rightarrow |G:3\mathbb{Z}| = 3$$

Index of H in K :-

$$3\mathbb{Z} = 15\mathbb{Z} \cup (3+15\mathbb{Z}) \cup (6+15\mathbb{Z}) \cup (9+15\mathbb{Z}) \cup (12+15\mathbb{Z}),$$

Since modulo 15, a multiple of 3, is congruent to 0, 3, 6, 9 or 12.

$$\therefore |H:K| = |3\mathbb{Z}:15\mathbb{Z}| = 5$$

Index of K in G :-

$15\mathbb{Z} = \{0, \pm 15, \pm 30, \dots\}$ for any integer $m \in \mathbb{Z}$, $m = 15q + r$, $0 \leq r \leq 14$.

$$\therefore 15\mathbb{Z} + m = 15\mathbb{Z} + r, \quad 0 \leq r \leq 14.$$

The cosets are $15\mathbb{Z}, 15\mathbb{Z}+1, \dots, 15\mathbb{Z}+14$.

$$\text{Hence } |G:K| = |G:15\mathbb{Z}| = 15$$

$$\text{Hence, } |\mathbb{Z}:3\mathbb{Z}| |3\mathbb{Z}:15\mathbb{Z}| = 3 \cdot 5 = 15 = |\mathbb{Z}:15\mathbb{Z}|$$

Example:-

Let H be a group of G and let $a, b \in G$. Show that aH and bH are distinct, if and only if Ha^{-1} and Hb^{-1} are distinct.

Solution:-

We know that two right cosets are either distinct or identical. If the right cosets Ha and Hb^{-1} are not distinct, then they will be identical, i.e. $Ha^{-1} = Hb^{-1}$.

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

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

and hence $H = (a^{-1}b)H$ [$\because Ha = H$ and $aH = H$, if $a \in H$]

Thus [$\because aH = bH \Leftrightarrow a^{-1}b \in H$ and $Ha = Hb \Leftrightarrow a^{-1}b \in H$]

But it is given that aH and bH are distinct.

Hence our assumption that $Ha^{-1} = Hb^{-1}$ is not correct.

Hence Ha^{-1} and Hb^{-1} are distinct.

Similarly it can be proved that if Ha^{-1} and Hb^{-1} are distinct, then aH and bH are distinct.

Example:-

Let H be a subgroup of G and let $a, b \in G$. Show that $aH = bH$ if and only if $Ha^{-1} = Hb^{-1}$.

Solution:-

We have $aH = bH$

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

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

$$\Leftrightarrow Ha^{-1}bH = HH = H$$

$$\Leftrightarrow Ha^{-1} = Hb^{-1}$$

Example:-

Suppose H and K are subgroups of a group and that $|H|$ and $|K|$ are relatively prime. Show that $H \cap K = \{e\}$.

Solution:- Since $H \cap K$ is a subgroup of a finite group H , we have $|H \cap K|$ divides $|H|$ by Lagrange's theorem.

Similarly, $|H \cap K|$ divides $|K|$.

As $|H|$ and $|K|$ are relatively prime i.e. $\gcd(|H|, |K|) = 1$,

this is possible only when $|H \cap K| = 1$ i.e. $H \cap K = \{e\}$.

MULTIPLICATION OF TWO SUBGROUPS:-

If H and K are the subgroups of the group G then their multiplication is a set denoted by HK .

where $HK = \{x \in G \mid x = hk, h \in H, k \in K\}$

By definition of HK , we know $hk \in HK \Rightarrow hk \in G$

$$\therefore HK \subseteq G$$

THEOREM:-

If H and K are any two subgroups of the group G then HK is subgroup iff $HK = KH$.

Proof:-

Condition necessary:-

Let HK is a subgroup of G .

Now let $x \in HK$
 $\Rightarrow x^{-1} \in HK$ ($\because HK$ is a subgroup)
 $\Rightarrow x^{-1} = hk$ for some $h \in H$ and $k \in K$
 $\Rightarrow (x^{-1})^{-1} = (hk)^{-1}$
 $\Rightarrow x = k^{-1}h^{-1}$

$$\therefore HK \subseteq KH \dots \dots (1)$$

Let $x \in KH$

$\Rightarrow x = kih_1$ for some $k_1 \in K, h_1 \in H$
 $\Rightarrow x^{-1} = (kih_1)^{-1}$
 $\Rightarrow x^{-1} = h_1^{-1}k_1^{-1}$
 $\Rightarrow x^{-1} \in HK$
 $\Rightarrow (x^{-1})^{-1} \in HK$ ($\because HK$ is a subgroup)
 $\Rightarrow x \in HK$

$$\therefore KH \subseteq HK \dots \dots (2)$$

From (1) and (2) we have,

$$HK = KH$$

Condition sufficient:-

Let $HK = KH$ is a subgroup. To prove HK is a subgroup of G , it is sufficient to show that HK obey closure and inverse axiom.

Closure axiom:-

Let $x, y \in HK$ $\exists x = h_1k_1$ and $y = h_2k_2$

$$\therefore xy = (h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2 \dots \dots (3)$$

Now $k_1h_2 \in KH$

$\Rightarrow k_1h_2 \in HK$ ($\because HK = KH$)

$$\text{Let } \exists h_3k_3 \in HK \text{ s.t. } h_3k_3 = k_1h_2 \dots \dots (4)$$

using (4) in (3), we have,

$$xy = h_1h_3k_3k_2 = (h_1h_3)k_3k_2 = h'k' \in HK$$

where $h' = h_1h_3 \in H$ and $k' = k_3k_2 \in K$

Hence closure axiom is satisfied.

inverse axiom:- Let $x = hk \in HK \Rightarrow x^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in KH$

$$\therefore x^{-1} \in KH$$

$\forall x^{-1} \in HK \quad (\because HK = KH)$

Hence inverse axiom is satisfied.

So HK is a subgroup.

Theorem:-

If H and K are the subgroups of the abelian group G , then HK is a subgroup.

Proof:-

Since H and K are the subgroups of the abelian group G then $HK = KH$.
To prove HK is a subgroup of G , it is sufficient to show that HK obeys closure and inverse axiom.

Closure axiom:-

Let $x, y \in HK \ni x = h_1 k_1$ and $y = h_2 k_2$

$$\therefore xy = (h_1 k_1)(h_2 k_2) = h_1 (k_1 h_2) k_2 \dots (1)$$

Now $k_1 h_2 \in KH$

$$\Rightarrow k_1 h_2 \in KH$$

$$\Rightarrow k_1 h_2 \in HK \quad (\because KH = HK)$$

$$\text{Let } \exists h_3 k_3 \in HK \ni h_3 k_3 = k_1 h_2 \dots (2)$$

using (2) in (1) we have

$$xy = h_1 (h_3 k_3) k_2 = (h_1 h_3) (k_3 k_2) = h k \in HK$$

where $h = h_1 h_3 \in H$ and $k = k_3 k_2 \in K$

Hence closure axiom is satisfied.

Inverse axiom:-

Let $x = h k \in HK$

$$\Rightarrow x^{-1} = (hk)^{-1} = k^{-1} h^{-1} \in KH$$

$$\therefore x^{-1} \in KH$$

$$\Rightarrow x^{-1} \in HK \quad (\because KH = HK)$$

$\therefore$ Inverse axiom is satisfied.

So HK is a subgroup.

Theorem:-

If H and K are finite subgroups of G of orders $o(H)$ and $o(K)$ respectively

$$\text{then } o(HK) = \frac{o(K) o(H)}{o(H \cap K)}$$

Proof:-

Since H and K are the finite subgroups of the group G then HK is a finite subset of G . As K is a subgroup of then by definition of subgroup K is itself a group. we know that intersection of two subgroups is a subgroup.

So $H \cap K$ is a subgroup. But $H \cap K \subset K$. Since K is the subgroup and $H \cap K \subset K$ then $H \cap K$ is a subgroup of K .

As K is finite then by Lagrange's theorem, $|o(H \cap K)| \mid |o(K)|$

Let $m = \frac{|o(K)|}{|o(H \cap K)|} = \frac{|o(K)|}{|o(T)|} \dots (1)$, where $T = H \cap K$

Hence m is the number of distinct right cosets of T in K .

Let $k_1, k_2, \dots, k_m$ are the elements of $K \ni Tk_1, Tk_2, \dots, Tk_m$ are the ' m ' distinct right cosets of T in K .

So $K = Tk_1 \cup Tk_2 \cup \dots \cup Tk_m$

$\Rightarrow K = \bigcup_{i=1}^m Tk_i$

$\Rightarrow HK = H\left(\bigcup_{i=1}^m Tk_i\right)$

$= \bigcup_{i=1}^m HTk_i$

$= \bigcup_{i=1}^m H(H \cap K)k_i \quad (\because T = H \cap K)$

$= \bigcup_{i=1}^m (HH)k_i \quad (\because H \cap K \subset H)$

$= \bigcup_{i=1}^m Hk_i \quad (\because HH = H)$

So $HK = Hk_1 \cup Hk_2 \cup \dots \cup Hk_m \dots (2)$

Now to prove each Hk_i are distinct cosets
 of possible let $Hk_i = Hk_j, i \neq j$

$\Rightarrow k_i k_j^{-1} \in H$

Again $k_i, k_j \in K \Rightarrow k_i, k_j^{-1} \in K \Rightarrow k_i k_j^{-1} \in K \quad (\because K \text{ is a subgroup})$

$\therefore k_i k_j^{-1} \in H \text{ and } k_i k_j^{-1} \in K$

$\therefore k_i k_j^{-1} \in H \cap K = T$

$\Rightarrow k_i k_j^{-1} \in T \Rightarrow Tk_i = Tk_j$ which is contradiction.

Since all the cosets of the type Tk_i are distinct. So our assumption is wrong.

$\therefore$ All the coset $Hk_1, Hk_2, \dots, Hk_m$ are distinct.

Hence the number of the elements in Hk_i is equal to the number of the elements in H .

$\therefore |o(Hk_i)| = |o(H)|$

$\therefore |o(HK)| = |o(Hk_1 \cup Hk_2 \cup \dots \cup Hk_m)| = m |o(H)| = \frac{|o(K)| |o(H)|}{|o(H \cap K)|} \text{ (using (1))}$

$\therefore |o(HK)| = \frac{|o(K)| \cdot |o(H)|}{|o(H \cap K)|}$

Corollary:-

If H and K are the subgroup of G and $|o(H)| \nmid |o(G)|, |o(K)| \nmid |o(G)|$ then $H \cap K \neq \{e\}$

Proof:- we know that for any subgroup H and K , HK is always a subset of G

$$\therefore H_K \subset G \Rightarrow o(H_K) \leq o(G) \dots \dots (1)$$

$$\text{we know, } o(H_K) = \frac{o(H) \cdot o(K)}{o(H \cap K)} \geq \frac{\sqrt{o(G)} \cdot \sqrt{o(G)}}{o(H \cap K)}$$

$$\Rightarrow o(H_K) \geq \frac{o(G)}{o(H \cap K)} \dots \dots (2)$$

combining (1) and (2) we get $o(G) \geq o(H_K) \geq \frac{o(G)}{o(H \cap K)}$

$$\Rightarrow o(G) \geq \frac{o(G)}{o(H \cap K)}$$

$\Rightarrow o(H \cap K)$ must be greater than 1.

$$\therefore o(H \cap K) \geq 2$$

$\Rightarrow H \cap K \neq \{e\}$ because order of $\{e\}$ is 1.