2.5 A counting principle :-

If H is a subgroup of G and $a \in G$, then Ha consists of all elements in G of the form 'ha' where $h \in H$.

If H, K are two subgroups of G, let

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

Lemma 2.5.1

HK is a Subgroup of G if and only if HK = KH.

proof:

First we take that HK = KH.

ie If $h \in H$ & $K \in H$, then $hK = k_1 h_1$ Some $k_1 \in K$, $h_1 \in H$.

To prove that HK is a subgroup of G.

ie we must verify that it is closed and every in HK has its inverse in HK.

Let's Show the closure first, so suppose $x = hK \in K$ and $y = h'k' \in Hx$.

Now, its enough to prove that $xy \in HK$.

Let $xy = hk\,h'k'$

Since $kh' \in KH = HK$

$\Rightarrow kh' \in HK$

$\Rightarrow kh' = h_2 k_2$ with $h_2 \in H_1$, $k_2 \in K_1$.

Hence $xy = h(kh')k'$

$= h(h_2 k_2)k' \Rightarrow (hh_2)(k_2 k')$

$\in HK$.

[$\because n \in H, h_2 \in H \Rightarrow hh_2 \in H$.

& $K_2 \in K$, $k' \in K \Rightarrow K_2 k' = K$].

ie $x \in HK$ & $y \in HK$

$\Rightarrow xy \in HK$

$\therefore$ HK is closed.

Also $x^{-1} = (hK)^{-1} \Rightarrow K^{-1}h^{-1}$

$\in KH = HK$

[$\because K^{-1} \in K, H^{-1} \in H \Rightarrow K^{-1}h^{-1} \in KH$]

ie $x^{-1} \in HK$

Thus HK is a Subgroup of G.

On the other hand,

If HK is a Subgroup of G, then to prove that $HK = KH$

For any $h \in H$, $k \in K$, $h^{-1}k^{-1} \in HK$.

Let us take $kh \in KH$ and

$kh = (h^{-1}k^{-1})^{-1}$ $\quad$ [$\because h^{-1}k^{-1} \in HK$, HK is a Subgroup of G. $\therefore (h^{-1}k^{-1})^{-1} \in HK$]

$\in HK$

Thus $KH \subset HK \rightarrow (1)$.

Now, if x is any element of HK.

$x^{-1} = hk \in HK$ and

$x = (x^{-1})^{-1} = (hk)^{-1}$

$= k^{-1}h^{-1}$ $\quad$ [$\because k^{-1} \in K, h^{-1} \in H, \Rightarrow k^{-1}h^{-1} \in KH$]

$\in KH$

i.e $x \in KH$

Thus $HK \subset KH \rightarrow (2)$

From (1) & (2) we get

$HK = KH$

Hence the proof.

2.4 Subgroups :-

Definition :-

A non empty subset H of a group G is said to be a subgroup of G if under the product in G, H it self forms a group.

Note:

1. If H is a subgroup of G and K is a subgroup of H then K is a subgroup of G.

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

3. The inverse of any element of a subgroup is same as the inverse of the same as an element of the group.

4. The order of any element of a subgroup is the same as the order of the element as a member of the group.

Examples :-

1. The multiplicative group $\{1, -1\}$ is a subgroup of the multiplicative group $\{1, -1, i, -i\}$.

2. The additive group of even integers is a subgroup of the additive group of all integers.

3. Let G be the group of non zero real numbers under multiplication and let H be the subset of positive rational numbers. Then H is a subgroup of G.

4. Let G be the group of all real numbers under addition, And Let H be the set of all integers. Then H is a subgroup of G.

5. Let G be the group of all real 2×2 matrix. $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $ab.bc \neq 0$ under matrix multiplication.

Let $H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G / ad \neq 0 \right\}$

Then H is a subgroup of G.

6. Let G be the group of all real 2×2 matrix. $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $ab-bc \neq 0$ under multiplication and let

$$H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \right\}$$

Then H is a subgroup of G.

7. Let G be the group of all non zero complex numbers $a+bi$ ($a,b \in R$, not both Zero) under multiplication and let $H = \{ a+bi \in G / a^2+b^2=1 \}$ Then H is a subgroup of G.

Lemma 2:4:1

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

i) $a,b \in H \Rightarrow ab \in H$ ii) $a \in H \Rightarrow a^{-1} \in H$.

proof:

If H is a subgroup of G.

Then H is closed w.r to multiplication,

$\therefore a \in H, b \in H. \Rightarrow ab \in H$

Let $a \in H$ and let a^{-1} be the inverse, let a in G Then the inverse of a in H is also a^{-1}

Each element of H must possess inverse.

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

Conversely,

Given (i), $a \in H, b \in H \Rightarrow ab \in H$

$\therefore$ H is closed w.r. to multiplication.

* The elements of H are also the elements of G.

Therefore the same composition must also be associative on H.

* The identity of the subgroup is the same as the identity of the group.

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

$\Rightarrow e \in H$ [using (i)]

$\therefore$ The identity of the group.

* Given (ii), $a \in H \Rightarrow a^{-1} \in H$

$\therefore$ Each element of H must possess inverse.

Hence H itself is a group for the composition in G. So H is a subgroup of G.

Lemma : 2.A.2 :

If H is a non empty finite subset of a group G and H is closed under multiplication, then H is a subgroup of G.

Proof:

It is given that H is closed w.r. to multiplication, i.e $a \in H, b \in H \Rightarrow ab \in H$.

Let $a \in H$, Then by the given condition $a^2 = aa \in H$, $a^3 = a^2 a \in H$, $a^4 = a^3 a \in H$ .... $a^m \in H$ where m is any +ve integer.

Thus the infinite collection of elements $a, a^2, a^3 \ldots a^m$, all belong to H.

But H is a finite subset of G (Given (i))

∴ There must be repitions in the Collection of elements. If they are all distinct, There B will not be a finite set.

∴ For some the integers r and s with $r > s > 0$, we must have $a^r = a^3$

$\Rightarrow a^r . a^{-3} = a^3 a^{-3}$ [$\because a^3 \in G \Rightarrow (a^3)^{-1} \in G$ i,e $a^{-3} \in G$]

$\Rightarrow a^{r-3} = a^0 = e$

$\therefore a^{r-3} = e \in H.$ Where e is identity of G.

∴ The identity e is also an element of G.

Now $r - s \geq 1$ $\therefore r - s - 1 \geq 0$

we have $a^{r-3-1} \in H$ and $a \in -H$

$\Rightarrow a\, a^{r-s-1} = a^{r-s} = e$

$\Rightarrow a^{-1} = a^{r-s-1}$

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

Finally, The element of H.are also the elements of G.

∴ H is associative.

Hence H is a Subgroup of G.

Theorem:

If H_1 and H_2 are two Subgroup of a group G. Then $H_1 \cap H_2$ is also a Subgroup of G.

Proof:

Let H_1, H_2 are two Subgroup of G.

Then $H_1 \cap H_2 \neq \phi$ since atleast the element e is common to Both.

we have to prove that $H_1 \cap H_2$ is a subgroup.

Now we enough to prove that

$a \in H_1 \cap H_2$, $b \in H_1 \cap H_2$, $ab^{-1} \in H_1 \cap H_2$

NOW $a \in H_1 \cap H_2 \Rightarrow a \in H_1$ and $a \in H_2$

$b \in H_1 \cap H_2 \Rightarrow b \in H_2$ and $b \in H_2$

But H_1, H_2 are subgroups.

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

$a \in H_2, b \in H_2 \Rightarrow ab^{-1} \in H_2 \rightarrow (2)$

From (1) & (2) we get

$ab^{-1} \in H_1 \cap H_2$

Thus we have shown that

$a \in H_1 \cap H_2$, $b \in H_1 \cap H_2 \Rightarrow a\cancel{b}^{-1} \in H_1 \cap H_2$
ab^{-1}

Hence $H_1 \cap H_2$ is a sub group of G.

Note:

The union of two subgroups is not necessary of a subgroup.

For ex: Let G be the additive group of Integers

Then $H_1 = \{\ldots -6, -4, -2, 0, 2, 4, 6, \ldots\}$

$H_2 = \{\ldots -12, -9, -6, -3, 0, 3, 6, 9 \ldots\}$

are both subgroups of G.

We have $H_1 \cup H_2 = \{-4, -3, -2, 0, 2, 3, 4, \ldots\}$

$\Rightarrow H_1 \cup H_2$ is not closed w.r. to addition.

Because $2 \in H_1 \cup H_2$, $3 \in H_1 \cup H_2$

But $2+3=5 \notin H_1 \cup H_2$

$\therefore H_1 \cup H_2$ is not a subgroup of G.

Theorem:

Show that the union of two subgroups is a subgroup iff one is contained in the G.

Proof:

Suppose H_1 and H_2 are two subgroups of G.

Let $H_1 \subseteq H_2$ (or) $H_2 \subseteq H_1$

Then $H_1 \cup H_2 = H_2$ (or) H_1

But H_1, H_2 are subgroups.

$\Rightarrow H_1 \cup H_2$ is also a subgroup.

Conversely, Suppose $H_1 \cup H_2$ is a subgroup

Prove that $H_2 \subseteq H_1$ (or) $H_1 \subseteq H_2$

Let us assume that H_1 is not a subgroup of H_2, and H_2 is not a subset of H_1

Now H_1 is not a subset of H_2.

$\Rightarrow \exists\ a \in H_1$ and $a \notin H_2$ $\longrightarrow$ ①

and H_2 is not a subset of H_1

$\Rightarrow \exists\ b \in H_2$ and $b \notin H_1$ $\longrightarrow$ ②

From ① & ②, we have $a \in H_1 \cup H_2$ & be

Since $H_1 \cup H_2$ is a subgroup.

$ab = c$ (say) $\in H_1 \cup H_2$

But $ab = c \in H_1 \cup H_2$

$\Rightarrow ab = c \in H_1$ or H_2

Suppose $ab = c \in H_1$

$b = a^{-1}c \in H_1$ $\quad [\because a \in H_1 \Rightarrow a^{-1} \in H_1]$

But from ②, $b \notin H_1$, we get a contradiction.

Again suppose $ab = c \in H_2$

Then $a = cb^{-1} \in H_2$ $\quad [\because b \in H_2 \Rightarrow b^{-1} \in H_2]$

But from ①, $a \notin H_2$

Thus here also we get a contradiction.

Hence either $H_1 \subseteq H_2$ (or) $H_2 \subseteq H_1$.

Definition:-

Let G be group, H a subgroup of G for $a, b \in G$, we say 'a' is congruent to 'b' mod H, i.e $a \equiv b \pmod H$ if $ab^{-1} \in H$.

Definition Equivalence Relations:-

Let R be a relation in a set A Then R is an equivalence relation in A iff

i) R is reflexive i.e $\forall a \in A$, aRa

ii) R is Symmetric i.e $aRb \Rightarrow bRa$

iii) R is transitive i.e aRb and $bRa \Rightarrow aRc$

This equivalence relation denoted by the symbol $\sim$.

Lemma: 2:4:3

The relation $a \equiv b \bmod H$ is an equivalence relation.

Proof:

For $a, b, c \in G$, we must verify the following three conditions.

1) $a \equiv a \bmod H$ (Reflexivity)

2) $a \equiv b \bmod H \Rightarrow b \equiv a \pmod H$ (Symmetry)

3) $a \equiv b \bmod H$, $b \equiv c \bmod H \Rightarrow a \equiv c \bmod H$ (Transitivity).

Reflexivity:

Let a be any element of G, Then $aa^{-1} = e$.

i.e $aa^{-1} = e \in H$. Since H is a subgroup of G.

$\therefore a \equiv a \bmod H$ for all $a \in G$

Hence the relation is reflexive.

Symmetry:

We have $a \equiv b \pmod H \Rightarrow ab^{-1} \in H$

$\Rightarrow (ab^{-1})^{-1} \in H$ [$\because H$ is a subgroup of G]

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

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

$\therefore$ The relation is symmetric.

Transitivity:

Let $a \equiv b \pmod H$ and $b \equiv c \pmod H$.

Then $ab^{-1} \in H$ and $bc^{-1} \in H$. But H is a subgroup

of G and thus H is closed w.r.to composition in G.

$\therefore (ab^{-1})(bc^{-1}) \in H$

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

$\Rightarrow a \equiv c \pmod{H}$

Hence the relation is transitive.

∴ The relation congruence mod H is an equivalence relation in G.

Definition : Cosets:

Suppose G is a group and H is any subgroup of G. Let $a \in G$, then the set $Ha = \{ha : h \in H\}$ is called the right coset of H in G.

Ily $aH = \{ah : h \in H\}$ is called the left coset of H in G.

Note:

1. If 'e' is the identity of G, then $He = H = eH$. Therefore H itself is a right as well as left coset.

2. If the composition in the group G has been denoted additively, then the right coset of H in G is defined as for any $a \in G$,

$$H+a = \{h+a : h \in H\}$$

similarly, left cost $a+H = \{a+h : h \in H\}$.

Example:

Let G be the additive group of integers.

i.e, $G = \{\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\}$

∴ Let H be the subgroup of G obtained on multiplying each element of G by 3

i,e $H = \{\ldots -9, -6, -3, 0, 3, 6, 9 \ldots\}$

Let us form the right cosets of H in G, we have $0 \in G$, and

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

$1 \in G$, and $H+1 = \{\ldots -8, -5, -2, -1, 0, 1, 4, 7, 10, \ldots\}$

$2 \in G$, and $H+2 = \{\ldots -7, -4, -1, 0, 5, 8, 11, \ldots\}$

$3 \in G$, and $H+3 = \{\ldots -6, -3, 0, 3, 6, 7 \ldots\}$

$= H$

$4 \in G$, and $H+4 = \{\ldots -8, -5, -2, 1, 4, 7, 10, \ldots\}$

$= H+1$

$5 \in G$, and $H+5 = \{\ldots -7, -4, -1, 0, 5, 8, 11, \ldots\}$

$= H+2$

11'y $H+6$, $H+(-1) = H+2$, $H+(-2) = H+1$ and so on.

Thus we get only three distinct right cosets i,e H, $H+1$, $H+2$ and

$G = H \cup (H+1) \cup (H+2)$.

Lemma : 2.4.4:

For all $a \in G$

$Ha = \{x \in G / a \equiv x \bmod H\}$.

Proof:

If $[a]$ is the equivalence class corresponding

to $a \in G$. Then we shall show that $[a] = Ha$.

By the definition of equivalence classes,

We have

$$[a] = \{x \in G / a \equiv x \bmod H\}$$

We first show that $Ha \subset [a]$

Let z be any arbitary element of Ha.

Then $z \in Ha$

$\Rightarrow za^{-1} \in Haa^{-1}$

$\Rightarrow za^{-1} \in He = H \Rightarrow za^{-1} \in H$

$\Rightarrow z \equiv a \pmod H \Rightarrow z \in [a]$

$\therefore Ha \subset [a]$

Now ~~that~~ let x be any arbitary element of $[a]$. Then

$x \in [a] \Rightarrow x \equiv a \bmod H$

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

$\Rightarrow xa^{-1}a \in Ha \Rightarrow xe \in Ha$

$\Rightarrow x \in Ha$

$\therefore [a] \subset Ha$

Hence $[a] = Ha$.

Theorem:

Any two right (left) cosets of a subgroup are either disjoint (or) identical.

Proof:

Suppose H is a subgroup of a group G and let Ha and Hb be two right cosets of H in G.

Suppose Ha and Hb are not disjoint. Then $\exists$ an element

$c \exists c \in Ha \wedge c \in$

Let $c = h_1 a$ and $c = h_2 b$ where $h_1, h_2 \in H$

Then $h_1 a = h_2 b$

$h_1^{-1} h_1 a = h_1^{-1} h_2 b$

$ea = h_1^{-1} h_2 b$

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

$a = h_3 b$

[$\because$ H is a subgroup of G

$h_2 \in H$. $h_1^{-1} \in H$

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

$\Rightarrow h_3 \in H$.

Now $Ha = Hh_3 b = (Hh_3) b$ [$\because h_3 \in H \Rightarrow Hh_3 = H$]

$Ha = Hb$

$\therefore$ The two right cosets are identical if they are not distinct.

Thus either $Ha \cap Hb = \phi$ (or) $Ha = Hb$.

Lemma : 2.4.5.

There is a one-to-one correspondence between any two right cosets of H in G.

Proof:

Let $a, b \in G$. Then Ha and Hb are any two right cosets of H in G.

Let $f: Ha \to Hb$ defined by

$f(ha) = hb \quad \forall\ h \in H$.

F is one-one:

If $h_1, h_2 \in H$ $\quad h_1 a, h_2 a \in Ha$

we have $f(h_1 a) = f(h_2 a)$

$h_1 b = h_2 b$ [by Right cancellation law].

$h_1 = h_2$

$h_1 a = h_2 a$.

$\therefore$ f is 1-1.

f is onto:

Let hb be any arbitrary element of Hb. Then

$hb \in Hb \Rightarrow h \in H$.

$ha \in Ha$

Now $f(ha) = hb$ by definition of f.

Thus $hb \in Hb \Rightarrow$ that there exists $ha \in Ha \ni f(ha) = hb$.

$\therefore$ f is onto.

Hence the proof.

Definition:

If H is a subgroup of G, the index of H in G is the number of distinct right cosets of H in G.

Lagrange's Theorem:

If G is a finite group and H is a subgroup of G, Then O(H) is a divisor of O(G).

Proof:

If G is a finite group and that H is a subgroup of G. Let $h_1, h_2, \ldots h_r$ be the r element of H.

i.e $O(H) = r$

If $H = G$, there is nothing to prove.

Suppose that $H \neq G$, Thus there is an element $a \in G$, $a \notin H$. List all the elements in the following two rows as

$h_1, h_2, \ldots h_r = H$

$h_1a, h_2a, \ldots h_ra = Ha$

We claim that all the entries in the second are

different from each other and are different from the entries in the first line.

Suppose if any two in the second line were equal.

i.e $h_i a = h_j a$ with $i \neq j$

$h_i = h_j$ [by cancellation law].

Which is contradiction.

∴ Ha has r distinct members.

suppose if an entry in the second line were equal to one in the first line.

i.e $h_i a = h_j$

$\Rightarrow a = h_i^{-1} h_j \in H$ [∵ H is a subgroup ∀ $h_j \in H$, $h_i^{-1} \in H \Rightarrow h_i^{-1} h_j \in H$.]

$\Rightarrow a \in H$

Which is a contradiction of $a \notin H$.

Thus we have listed 2.o(H) elements. If these elements don account for all the element of G.

If not, there is $a, b \in G$ which did not occur in these two lines.

consider the new list,

$h_1, h_2, \ldots h_r = H$

$h_1 a, h_2 a, \ldots h_r a = Ha$

$h_1 b, h_2 b, \ldots h_r b = Hb$

AS before we could show that no two entries in the third line are equal to each other, and that no entry in the third

line occurs in the 1st or 2nd line.

Thus we have listed 3.O(H) elements continuing in this way, every element introduced, produces O(H) new elements.

Since G is a finite group, The number of distinct right cosets of H in G will be finite, say equal to K.

The union of these K distinct right cosets of H in G is equal to G.

i.e $G = Ha \cup Hb \cup Hc \cup \ldots$ K times

$$O(G) = K \cdot O(H)$$

$$K = \frac{O(G)}{O(H)}$$

$\Rightarrow O(H)$ is a divisor of $O(G)$.

Hence the theorem.

Corollary:

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

Proof:

We know that if H, K are two subgroups of a group G, then HK is a subgroup of G. If and only if $HK = KH$.

∴ Since the given group G is here abelian, therefore we have $HK = KH$.

Hence HK is a subgroup of G.

Theorem : 9.5.1.

If H and K are finite subgroups of G of orders $O(H)$ and $O(K)$ respectively, then

$$O(HK) = \frac{O(H)\,O(K)}{O(H \cap K)}.$$

Proof:

Let $h \in H$, $k \in K$ so that $hk \in HK$

Here we should seek to show that

$O(HK) = O(H)\,O(K)$. Let us take $H \cap K = (e)$

Now, if we list all the elements $hk \in HK$,

$h \in H$, $k \in K$

Suppose that there should be some collapsing i.e, some elements in the list must appear atleast twice.

For, some $h \neq h_1 \in H$, $hk = h_1 k_1$

$\Rightarrow h_1^{-1} hk = h_1^{-1} h_1 k_1$

$\Rightarrow h_1^{-1} hk = e k_1$

$\Rightarrow h_1^{-1} h k k^{-1} = k_1 k^{-1}$

$\Rightarrow (h_1^{-1} h) e = k_1 k^{-1}$

$\Rightarrow h_1^{-1} h = k_1 k^{-1}$

[$\because h_1 \in H$ & $h_1^{-1} \in H$]

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

$\Rightarrow k_1 \in K$, $k^{-1} \in K$

$\Rightarrow k_1 k^{-1} \in K$.

Thus $h_1^{-1} h \in H$ & $k_1 k^{-1} \in K$

$\therefore h_1^{-1} h = k_1 k^{-1} \in H \cap K = (e)$

so that $h_1^{-1} h = e \Rightarrow h = h_1$

which is contradiction.

$\therefore$ We can proved that no collapsing can occur.

$\therefore \quad O(H) = O(H)\, O(K)$

In general case, as above a given element hk appears as a product in the list of HK it must appear $O(H \cap K)$ times.

TO see that if $h_1 \in H \cap K$ Then $hk = (hh_1)(h_1^{-1}k)$

Where $hh_1 \in H$, Since $h \in H$, $h_1 \in H \cap K \subset H$ and $h_1^{-1} \in K$, Since $h_1^{-1} \in H \cap K \subset K$ & $k \in K$.

Thus hk is duplicated in the product atleast $O(H \cap K)$ times.

However, not all symbols need represent distinct group elements.

i.e we may ~~here~~ have $hk = h'k'$

then $h^{-1} h k = h^{-1} h' k'$

$$k = h^{-1} h' k'$$

$$kk' = (h^{-1}h')\, k' k^{-1}$$

$\Rightarrow kk^{-1} = h^{-1}h' = u$ and $u \in H \cap K$ so that

$h' = hu$, $k' = u^{-1}k$

Thus each element in HK is represented by at lest $O(H \cap K)$ products in HK. Thus the number of distinct elements in HK is the total number of elements in ~~HK~~ HK. i.e $O(H)\, O(K)$, divided by the number of times a given element appears namely $O(H \cap K)$.

i/e $O(HK) = \frac{O(H) \cdot O(K)}{O(H \cap K)}$

Hence the proof.

Proof:

HK is a subset of G it is not necessary that it will be a subgroup of G By O(HK) we mean the number of distinct elements in HK.

Let $D = H \cap K$ Then D is a subgroup of G and $D \subseteq K$. Therefore D is a subgroup of K. Since K is finite.

The number of distinct rights cosets in the right coset decomposition of K with respect to 'D' is finite.

Let it be 'm' By using Langrange's theorem,

We have $m = \frac{O(K)}{O(D)}$.

If $DK_1, DK_2, \ldots DK_m$ are the distinct right cosets of D in K, then

$$K = DK_1 \cup DK_2 \cup \ldots \cup DK_m = \bigcup_{i=1}^{m} DK_i$$

Observe that $k_1, k_2, \ldots k_m$ are same distinct elements in K.

Now $HK = H\left(\bigcup_{i=1}^{m} DK_i\right) = \bigcup_{i=1}^{m} H\,DK_i$

$= \bigcup_{i=1}^{m} HK_i$ $\quad [\because D \subseteq H \Rightarrow HD = H]$

$= HK_1 \cup HK_2 \cup \ldots \cup HK_m \longrightarrow (1)$

we shall show that the cosets

$Hk_1, Hk_2, \ldots Hk_m$ are positive pairwise distinct

we have,

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

$\Rightarrow k_i k_j^{-1} \in H \cap K \quad [\because k_i k_j \in K \Rightarrow k_i k_j^{-1} \in K]$.

$\Rightarrow k_i k_j^{-1} \in D \Rightarrow Dk_i = Dk_j$

$\Rightarrow k_i = k_j \quad [\because Dk_1 \ldots Dk_m$ are distinct cosets$]$.

Thus $Hk_1, Hk_2, \ldots Hk_m$ are distinct right cosets and so they are pairwise distinct also

The number of elements in each of them is equal to $O(H)$.

i.e The number of elements in H.

$\therefore$ From (1), we conclude that the number of elements in HK is equal to $m \cdot O(H)$.

$\therefore O(HK) = m \cdot O(H)$

$= \frac{O(K)}{O(D)} \cdot O(H) \quad \left(\because m = \frac{O(K)}{O(D)}\right)$.

$= \frac{O(H) \cdot O(K)}{O(D)}$

(i.e) $O(HK) = \frac{O(H) \cdot O(K)}{O(H \cap K)}$

corollary:

Let H and K be subgroups of a finite group G and let $O(H) > \sqrt{O(G)}$, $O(K) > \sqrt{O(G)}$ Then $H \cap K \neq \{e\}$.

Proof:

Suppose H, K are subgroups of the finite group G and $O(H) > \sqrt{O(G)}$, $O(K) > \sqrt{O(G)}$

Since $HK \subset G$, $O(HK) \leq O(G)$

However, $O(G) \geq O(HK)$

$$\geq \frac{O(H)\,O(K)}{O(H \cap K)} > \frac{\sqrt{O(G)}\,\sqrt{O(G)}}{O(H \cap K)}$$

$$O(G) > \frac{O(G)}{O(H \cap K)}$$

$$\Rightarrow O(H \cap K) > \frac{O(G)}{O(G)}$$

Thus $O(H \cap K) > 1 \quad \therefore H \cap K \neq (e)$.

Example:

Let G be a finit group of order pq where p and q are prime numbers wit $p \geq q$. Then G has at most one subgroup of order p.

Solution:

Suppose G is a finite group of order pq. where p and q are prime numbers with $p \geq q$.

We claim that G can have almost one subgroup of order p.

For, suppose H, K are subgroups of order p. By the corollary $HnK \neq (e)$ and being a subgroup of H, which having prime order has no nontrivial subgroups.

We must conclude that $H \cap K = H$

and so $H < H \cap K \subset K$

similarly $K \subseteq H$

Hence $H = K$

$\therefore$ There can be at most one subgroup of order p.

Definition: (Normalizor of an element of a group).

If $a \in G$, then $N(a)$, the Normalizer of 'a' in G is the set of all those elements of G which commute with a symbolically.

$N(a) = \{ x \in G / ax = xa \}$.

Theorem:

The Normalizer $N(a)$ is a subgroup of G.

proof:

We have $N(a) = \{ x \in G / ax = xa \}$

Let $x_1, x_2 \in N(a)$. Then $ax_1 = x_1 a$, $ax_2 = x_2 a$ First we show that $x_2^{-1} \in N(a)$

we have $ax_2 = x_2 a \Rightarrow x_2^{-1}(ax_1)x_2^{-1} = x_2^{-1}(x_2 a)x_2^{-1}$

$\Rightarrow (x_2^{-1}a)(x_2 x_2^{-1}) = (x_2^{-1}x_2)(x_2 a x_2^{-1})$

$\Rightarrow x_2^{-1}a = ax_2^{-1}$

$\Rightarrow x_2^{-1} \in N(a)$

Now we shall show that $x_1 x_2^{-1} \in N(a)$

we have $a(x_1 x_2^{-1}) = (ax_1)x_2^{-1} = (x_1 a)x_2^{-1}$

$= x_1(ax_2^{-1}) = x_1(x_2^{-1}a)$

$= (x_1x_2^{-1})a$

$\therefore x_1x_2^{-1} \in N(a)$

Thus $x_1, x_2 \in N(a) \Rightarrow x_1x_2^{-1} \in N(a)$

$\therefore N(a)$ is a subgroup of G.

Definition: (Center of a group)

Centre of a group is a set of all elements of G, which are commutative with each and every element of G.

i.e $Z = \{x \in G / zx = xz \ \forall x \in G\}$.

Theorem:

The centre of a group is subgroup of G.

Proof:

we have $Z = \{z \in G / zx = xz \ \forall x \in G\}$ we shall have Prove that Z is a subgroup of G.

Let $z_1, z_2 \in Z$

Then $z_1x = xz_1$ & $z_2x = xz_2$, for all $x \in G$

we have $z_2x = xz_2 \quad \forall x \in G$

$\Rightarrow z_2^{-1}(z_2x)z_2^{-1} = z_2^{-1}(xz_2)z_2^{-1}$

$\Rightarrow xz_2^{-1} = z_2^{-1}x \quad \forall x \in G$

$\Rightarrow Z_2^{-1} \in Z$

Now, $(Z_1 Z_2^{-1})x = Z_1(Z_2^{-1}x) = Z_1(xZ_2^{-1})$

$= (Z_1 x)Z_2^{-1} = (xZ_1)Z_2^{-1}$

$(Z_1 Z_2^{-1})x = x(Z_1 Z_2^{-1})$

$\therefore Z_1 Z_2^{-1} \in Z$

Thus $Z_1, Z_2 \in Z \Rightarrow Z_1, Z_2^{-1} \in Z$.

$\therefore Z$ is a subgroup of G.

2.6 Normal subgroups & Quotient Groups.

Definition : Normal subgroup:

A subgroup N of G is said to be normal subgroup of G if for every $g \in G$ and $n \in N$, $gng^{-1} \in N$.

We see that N is a Normal subgroup of G if and only if $gNg^{-1} \subset N$ for every $g \in G$.

Lemma 2.6.1.

N is a normal subgroup of G if and only if $gNg^{-1} = N$ for every $g \in G$.

Proof:

If $gNg^{-1} = N$ for every $g \in G$

Then $gNg^{-1} \subset N \quad \forall\ g \in G$

$\therefore N$ is a Normal subgroup of G.

converse:

Let N is a Normal subgroup of G

Then $gNg^{-1} \subset N \quad \forall\ g \in G \rightarrow (1)$

Also $g \in G \Rightarrow g^{-1} \in G$

$\therefore$ we have $g^{-1}Ng = g^{-1}N(g^{-1})^{-1} \subset N \quad \forall\ g \in G$

$\Rightarrow g(g^{-1}Ng)g^{-1} \subset gNg^{-1} \quad \forall\ g \in G$

$\Rightarrow N \subset gNg^{-1}$ for all $g \in G \rightarrow (2)$

From (1) & (2) we get $gNg^{-1} = N$ for all $g \in G$.

Lemma : 2.6.2.

The subgroup N of G is normal subgroup of G if and only if every left coset of N in G is a right coset of N in G.

Proof:

Let N be a Normal Subgroup of G

Then $gNg^{-1} = N \quad \forall\ g \in G$

$\Rightarrow (gNg^{-1})g = Ng$ for all $g \in G$

$\Rightarrow (gN)(g^{-1}g) = Ng$

$\Rightarrow gN = Ng$ for all $g \in G$.

converse

Suppose that every left coset of N in G is a right coset of N in G.

Let g be any element of G,

Then $gN = Ng^{-1}$

Since $e \in N$, therefore $ge = g \in gN$

$\therefore g \in Ng'$ [$\because gN = Ng'$]

But $g \in Ng' \Rightarrow Ng = Ng'$ [$\because g, g' \in G$, N is subgroup of G.

$\therefore Ng = gN$ [$\because Ng' = gN$] $\Rightarrow g \in Ng' \Leftrightarrow Ng = Ng'$

Thus we have

$gN = Ng \quad \forall \; g \in G \Rightarrow gNg^{-1} = Ngg^{-1} \quad \forall g \in G$

$\Rightarrow gNg^{-1} = N \quad \forall \; g \in G$

$\Rightarrow N$ is a normal subgroup of G.

Theorem:-

If H is any subgroup of a group G, then $HH = H$.

Proof:

Let $h_1 h_2$ be any element of HH, where $h_1, h_2 \in H$.

$\therefore h_1 h_2 \in H \Rightarrow h_1 h_2 \in H$. [$\because H$ is a subgroup]

$\therefore HH \subset H \rightarrow (1)$

Now let h be any elements of H. Then we can write $h = he$, where e is identify of G.

Now $he \in HH$ [$\because h \in H, e \in H$]

Thus $H \subset HH \rightarrow (2)$

From (1) & (2) we get

$HH = H$

Lemma 2:6:8:

A subgroup N of G is a normal subgroup of G if and only if the product of two right cosets of N in G is again a right coset of N in G.

Proof:

Let N be a normal subgroup of a group G. Let a, b be any two elements of G.

Then Na and Nb are two right cosets of N in G.

We have $(Na)(Nb) = N(aN)b$

$= N(Na)b$ [$\because$ N is normal $\Rightarrow Ha = aH$]

$= NNab$

$= Nab$ [$\because HH = H$]

$\therefore Nab$ is also a right coset of N in G. Thus the product of the right cosets Na and Nb is the right coset Nab.

Converse:

Let N be a subgroup of G such that the product of two right cosets of N in G is again a right coset of N in G.

Let $g \in G$ Then $\exists\ g^{-1} \in G$

$\therefore Ng$ and Ng^{-1} are two right cosets of N in G

$\therefore NgNg^{-1}$ is also a right coset of N in G. [Given]

Let us take $ege^{-1} = e$ is an element of right coset $NgNg^{-1}$ $\therefore [e \in N]$

But N itself is a right coset of N in G and $e \in N$.

But we know that if any two right cosets have one element common they must be identical.

$\therefore Ngn^{-1} = N \quad \forall g \in G$

$\Rightarrow n_1 g n g^{-1} \in N \quad \forall g \in G, \forall n_1, n \in N$

$\Rightarrow n_1^{-1}(n_1 g n g^{-1}) \in n_1^{-1} N \quad \forall g \in G \; \forall n_1, n \in N.$

$\Rightarrow (n_1^{-1} n_1)(gng^{-1}) \in N \quad [\because n_1^{-1} \in N \Rightarrow n_1^{-1} N = N]$

$\Rightarrow gng^{-1} \in N$

$\Rightarrow$ N is normal subgroup.

Theorem :-

Every subgroup of an abelian group is normal

Proof:

Let G be an abelian group and N a subgroup of G.

Let g be any element of G and n be any element of N.

We have $gng^{-1} = gg^{-1}n \quad [\because G \text{ is abelian} \Rightarrow ng^{-1} = g^{-1}n]$

$= n \in N$

Thus $g \in G, n \in N \Rightarrow gng^{-1} \in N$

Hence N is Normal Subgroup.

Note:

* Every cyclic group is abelian
* Every subgroup of a cyclic group is normal.

Definition:

Any non empty subset H of a group G is called a complex of the group G.

Example:

If H is a subgroup of G and N is normal subgroup of G, show that $H \cap N$ is normal subgroup of H.

Solution:

Since H and N are subgroup of G.

$\therefore H \cap N$ is also a subgroup of G.

we have $H \cap N \subset H$.

$\therefore H \cap N$ is a subgroup of H.

Now to show that $H \cap N$ is normal subgroup of H.

Let g be any element of H and n be any element of $H \cap N$.

Then $g \in H$, $n \in N$.

$\Rightarrow gng^{-1} \in N$ [$\because$ N is normal]

Also H is a subgroup of G.

$\therefore$ we have $g \in H$, $n \in H \Rightarrow gng^{-1} \in H$.

Thus $gng^{-1} \in H \cap N$.

$\therefore H \cap N$ is normal subgroup of G.

Example 6:

Show that a normal ~~complex~~ subgroup is commutative with every complex.

Solution:

Suppose N is a normal subgroup and H is any complex of a group G. Then to prove that $HN = NH$.

Let $nh \in NH$ where $n \in N$, $h \in H$. we can write $nh = hh^{-1}nh$

$= h(h^{-1}nh)$. But N is a normal subgroup. Therefore $h^{-1}nh \in N$. Hence $nh \in HN$. Therefore $NH \subseteq HN$.

Again let $hn \in HN$ where $h \in H$, $n \in N$, We can write $hn = (hnh^{-1})h$. But $hnh^{-1} \in N$ because N is normal in G.

Therefore $hn \in NH$. Thus $HN \subseteq NH$. Hence $HN = NH$.

Example: 7

If N is a normal subgroup of G and H is any subgroup of G, Prove that NH is a subgroup of G.

Solution:

We know that a normal subgroup is commutative with every complex.

Since N is a normal subgroup of G and H is any subgroup of G, therefore we must have $NH = HN$. Now N and H are two subgroups of G. Such that $NH = HN$. Therefore NH is also a subgroup of G.

Example : 8

If H is a subgroup of G and N is a normal subgroup of G, such that

i) HN is a subgroup of G.

ii) N is a normal subgroup of HN.

Solution :-

i) Proceed as in Ex-7.

ii) Since $e \in H$, Therefore obviously $N \subseteq HN$. Because if $n \in N$, then we can write $n = en$ which is an element of HN.

Now, HN is a subgroup of G and N is also a subgroup of G. Also $N \subseteq HN$. Therefore N is a subgroup of HN. Now to show that N is a normal subgroup of HN. Let $h_1 n_1$ be any element of HN. and n be any element of N. Then $h_1 \in H, n_1 \in N$ and we have $(h_1 n_1) n (h_1 n_1)^{-1} = h_1 (n_1 n n_1^{-1}) h_1^{-1} \in N$ since N is normal in G and $n_1 n n_1^{-1} \in N, h_1 \in G$. Therefore N is a normal subgroup of HN

Example 9:

If N and M are normal subgroups of G, prove that NM is also a normal subgroup of G.

Solution:

We know that a normal subgroup is commutative with every complex. Therefore we have $NM = MN$. Now N and M are two subgroups of G such that $NM = MN$. Therefore NM is a subgroup of G.

Now to show that NM is normal subgroup of G. Let x be any element of G and nm be any elements of NM. Then $n \in N$, $m \in N$ and we have

$x(nm)x^{-1} = (xnx^{-1})(xmx^{-1})$ $\in NM$.

($\because$ N is normal $\Rightarrow xnx^{-1} \in N$ and M is normal $\Rightarrow xmx^{-1} \in M$]

Hence NM is a normal subgroup of G.

Example 10:

Suppose that N and M are two normal subgroups of G and then $N \cap M = (e)$. Show that every element of N commutes with every element of M.

Solution:

Let n be any element of N and m any element of M. Then to prove that $nm = mn$. consider the element $nmn^{-1}m^{-1}$

$\therefore$ Since N is Normal, $mn^{-1}m^{-1} \in N$, Also $n \in N$. Therefore $nmn^{-1}m^{-1} \in N$

Again M is normal $\Rightarrow nmn^{-1} \in M$. Also $m^{-1} \in M$. Therefore $nmn^{-1}m^{-1} \in N$. Thus

$nmn^{-1}m^{-1} \in N$ and $nmn^{-1}m^{-1} \in M$.

$\Rightarrow nmn^{-1}m^{-1} \in N \cap M$

$\Rightarrow mnn^{-1}m^{-1} = e$

$\Rightarrow nm = mn$.

[$\because (e) = N \cap M$]

Example: 11:

Let G be a group, H a subgroup of G. Let, for $g \in G$, $gHg^{-1} = [ghg^{-1} : h \in H]$ prove that gHg^{-1} is a subgroup of G.

Solution:

Let gh_1g^{-1}, gh_2g^{-1} be any two element of gHg^{-1}

Then $h_1, h_2 \in H$. Also we have

$(gh_1g^{-1})(gh_2g^{-1}) = gh_1g^{-1}(g^{-1})^{-1}h_2^{-1}.g^{-1} = gh_1g^{-1}gh_2^{-1}g^{-1}$

$= gh_1h_2^{-1} \in gHg^{-1}$ since $h_1h_2^{-1} \in H$

$\therefore gHg^{-1}$ is a subgroup of G.

Example 19:

Suppose H is the only subgroup of finite order m in the group G. Prove that H is a normal subgroup of G.

Solution:

H is a subgroup of G and $o(H) = m$. If x is any element of G then as in Ex. 11. xHx^{-1} is also a subgroup of G.

Then $xHx^{-1} = (xh_1x^{-1}, xh_2x^{-1}, \ldots xh_mx^{-1})$

The number of distinct elements in xHx^{-1} is m because

$xhx^{-1} = xh_1x^{-1} \Rightarrow h_1 = h_1$

$\therefore o(xHx^{-1}) = o(H) = m.$

But H is the only subgroup of G of order m. Therefore we must have $xHx^{-1} = H \quad \forall x \in G$, Hence H is a normal subgroup of G.

Quotient Group.

Definition:

If G is a group, and N is a normal subgroup of G. then the set G/N of all cosets of N in G is a group. It is called the quotient group or factor group of G by N.

* The identity element of G/N is N.

Theorem : 2:6:1.

If G is a group, N a normal subgroup of G, then G/N is a group.

proof:

Let G/N denote the collection of eight coset of N in G.

We have to prove that G/N is a group, Let us define $G/N = \{Na / a \in G\}$.

1. closure:

Let $x, y \in G/N \Rightarrow xy \Rightarrow G/N$

For Let $x \Rightarrow Na$, $y = Nb$ for some $a, b \in G$ and *

$xy = NaNb = Nab \in G/N$.

2. Associativity:

Let $x, y, z \in G/N$ then $x = Na$, $y = Nb$, $z = Nc$ with $a, b, c \in G$.

$(xy)z = (NaNb)Nc = (Nab)Nc = N(ab)c$

$= Na(bc) = Na(Nbc) = Na(NbNc) = x(yz)$.

Thus the product in G/N satisfies the associative law.

3. Existence of identity:

Consider the element N, $Ne \in G/N$

If $x \in G/N$, $x = Na$ for some $a \in G$.

Then $xN = NaNe = Nae = Na = x$

Similarly, $Nx = x$

$\therefore Ne$ is a identity element for G/N.

4. Existence of inverse:

Suppose $x = Na \in G/N$ for some $a \in G$, Thus $Na^{-1} \in G/N$

we have $NaNa^{-1} = Naa^{-1} = Ne$

Similarly $Na^{-1}Na = Ne$

Hence Na^{-1} is the inverse of Na in G/N.

Hence G/N is a group.

Lemma : 2.6.4:

If G is a finite group and N is a normal subgroup of G, the $o(G/N) = o(G)/o(N)$.

Proof:-

we have, $o(G/N)$ is the Number of distinct right coset of N in G.

i.e index of N in G

$$i_G(N) = o(G)/o(N).$$

$i_G(N)$

$$O(G/N) = \frac{\text{Number of elements in } G}{\text{number of elements in } N}$$

[by Lagrange's theorem]

$$= \frac{O(G)}{O(N)}.$$

Example :

show that every quotient group of an abelian group is abelian.

Solution:

Let G be an abelian group and N be normal subgroup of G.

If $a, b \in G$, Then Na, Nb are any two elements of G/N.

we have $(Na)(Nb) = N(ab) = N(ba)$

$= (Nb)(Na)$ [$\because$ G is abelian $ab = ba$]

$\therefore G/N$ is abelian.

2.7. Homomorphisms.

Definition :- (Homomorphism):

A mapping ϕ from a group G into a group $\bar{G}$ is said to be a homomorphism if for all $a, b \in G$,

$\phi(ab) = \phi(a) \cdot \phi(b)$.

Example :

1. $\phi(x) = e$ all $x \in G$ is a trivial homomorphism.
2. $\phi(x) = x$ for every $x \in G$ is a homomorphism.
3. Let Q be the group of all real number under addition

and let $\overline{G}$ be the group of non zero real Numbers with the product being ordinary multiplication of real numbers and

$\phi : G \to \overline{G}$ is defined by for every $x \in G$

$\therefore \phi(x) = 2^x$ is a homomorphism of G in to $\overline{G}$. but not onto $\overline{G}$.

$$\phi(x+y) = 2^{x+y} = 2^x \cdot 2^y = \phi(x)\,\phi(y).$$

4. Let G be the group of integers under addition and let $\overline{G} = \circ G$.

For the integer $x \in G$ define ϕ by $\phi(x) = 2x$.

$$\phi(x+y) = 2(x+y) = 2x+2y$$

$$\phi(x+y) = \phi(x) + \phi(y)$$

i.e ϕ is homomorphism of G.

5- Let G be the group of non zero real numbers under multiplication, $\overline{G} = \{1, -1\}$.

Define $\phi : G \to \overline{G}$ by $\phi(x) = 1$ if x is +ve

$= -1$ if x is -ve.

Which is a homomorphism G onto $\overline{G}$.

Lemma 2:7:1

Suppose G is a group, N a normal subgroup of G, define the mapping ϕ from G to G/N by $\phi(x) = Nx$ for all $x \in G$. Then ϕ is a homomorphism of G onto G/N.

proof:

Define mapping $\phi : G \to G/N$ is defined by

$\phi(x) = Nx$ for all $x \in G$.

This function ϕ y onto is trivial. For every element $X \in G/N$ is of the form $X = Ny$, $y \in G$. So $X = \phi(y)$

If $x, y \in G$,

$\phi(xy) = Nxy = Nx.Ny = \phi(x)\,\phi(y)$.

Hence ϕ is a homomorphism of G onto G/N.

Definition: (Kernel of a homomorphism):

If ϕ is a homomorphism of G into $\bar{G}$, the Kernel of ϕ, $K\phi$ is defined by.

$K\phi = \{x \in G \,(\, \phi(x) = \bar{e}, \bar{e} = \text{identity element of } \bar{G}\}$.

Lemma 2:7:2

If ϕ is a homomorphism of G into $\bar{G}$. Then

1. $\phi(e) = \bar{e}$, the unit element of $\bar{G}$
2. $\phi(x^{-1}) = \phi(x)^{-1}$ for all $x \in G$.

Proof:

1. Let $\phi(x)\bar{e} = \phi(x) = \phi(xe)$

$\Rightarrow \phi(x)\bar{e} = \phi(x)\phi(e)$

using cancellation laws

$\bar{e} = \phi(e)$

ie $\phi(e) = \bar{e}$

2. we know that

$\bar{e} = \phi(e) = \phi(x x^{-1}) = \phi(x)\phi(x^{-1})$

i.e $\phi(x)\,\phi(x^{-1}) = \bar{e}$

By the definition given by $\phi(x)^{-1}$ in $\bar{G}$.

$\therefore \phi(x^{-1}) = \phi(x)^{-1}$

Lemma 2.7.3:

If ϕ is a homomorphism G into $\bar{G}$ with kernel K, then K is a normal subgroup of G.

Proof:

First we show that K is a subgroup of G.

i.e we have to prove that K is closed under multiplication and has inverses for every element belongs to K.

1. closure:

If $x, y \in K$, then $\phi(x) = \bar{e}$, $\phi(y) = \bar{e}$.

where $\bar{e}$ is the identity element of $\bar{G}$.

So, $\phi(xy) = \phi(x)\,\phi(y)$ [$\because \phi$ is homomorphism].

$= \bar{e}.\bar{e}$

$= \bar{e}$

Here $xy \in K$.

2. Inverse:

Also if $x \in K$, then $\phi(x) = \bar{e}$. Already we know that

$\phi(x^{-1}) = \phi(x)^{-1}$

$= (\bar{e})^{-1} = \bar{e}$

(i.e) $\phi(x^{-1}) = \bar{e}$

$\Rightarrow x^{-1} \in K$

From 1 and 2 we get K is Subgroup of G.

Next we prove that K is normal Subgroup of G.

For any $g \in G$, $R \in K$, Then

$\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1})$ [$\because \phi$ is homo ϕ]

$= \phi(g)\bar{e}\phi(g^{-1})$ [$\because k \in K \Rightarrow \phi(k) = \bar{e}$]

$= \phi(g)\phi(g^{-1})$ [$\because \phi(g^{-1}) = \phi(g)^{-1}$]

$= \phi(g)\phi(g)^{-1}$

$\therefore \phi(gkg^{-1}) = \phi(g)\phi(g^{-1})$

$= \bar{e}$.

$\Rightarrow gkg^{-1} \in K$.

$\therefore K$ is normal Subgroup of G.

Hence the proof.

Lemma 2:7:4:

If ϕ is a homomorphism of G onto $\bar{G}$ with Kernel K, then the set of all inverse images of $\bar{g} \in \bar{G}$ under ϕ is is given by Kx. where x is any particular inverse image of $\bar{g}$ in G.

Proof:

Let ϕ is a homomorphism of G onto $\bar{G}$ and K is kernel of ϕ.

Let $g \in G$ and $\phi(x) = \bar{g} \in \bar{G}$.

we have to prove that $\phi(x) = \bar{g} = Kx$.

Let $y \in Kx$, Then $y = kx$ for some $k \in K$.

We have $\phi(y) = \phi(kx)$

$\Rightarrow \phi(y) = \phi(k)\phi(x)$ $\quad [\because k \in K \Rightarrow \phi(k) = \bar{e}]$.

$= \bar{e}\,\phi(x)$

$= \phi(x)$

$= \bar{g}$.

Thus all the elements kx all in the inverse image of $\bar{g}$ for any $x \in G$.

Let us suppose that $\phi(z) = \bar{g} = \phi(x)$

$\Rightarrow \phi(z) = \phi(x)$

$\Rightarrow \phi(z)\phi(x)^{-1} = \bar{e}$ $\quad [\because \phi(x)^{-1} = \phi(x^{-1})]$

$\Rightarrow \phi(z)\phi(x^{-1}) = \bar{e}$

$\Rightarrow \phi(zx^{-1}) = \bar{e}$ $\quad [\because \phi$ is homomorphism$]$

$\Rightarrow zx^{-1} \in K$.

$\Rightarrow z \in Kx$.

we have shown that kx is the all the inverse image of $\bar{g}$ and x is a particular inverse image of $\bar{g}$ in G.

Definition: (Isomorphism):

A homomorphism ϕ from G into $\bar{G}$ is said to be a Isomorphism if ϕ is one-to-one.

Definition :- (Isomorphic) :

A homomorphism ϕ from G into $\bar{G}$ is said to be isomorphic if there is an isomorphism of G onto $\bar{G}$.

i.e we write $G \cong \bar{G}$.

Corollary :-

A homomorphism ϕ of G into $\bar{G}$ with Kernel K_ϕ is an isomorphism of G into $\bar{G}$ if and only if $K_\phi = (e)$.

Proof :-

Let ϕ be a homomorphism of G into $\bar{G}$ Then ϕ is one-to one.

Now we prove that $K_\phi = (e)$.

Let $x \in K$. Then $\phi(x) = \bar{e}$

$\Rightarrow \phi(x) = \phi(e)$ $\quad [\because \phi(e) = \bar{e}]$

$\Rightarrow x = e$.

Thus $x \in K \Rightarrow x = e$.

$\therefore e$ is the only element of G which belongs to K.

$\therefore K_\phi = (e)$.

Converse :-

Suppose that $K_\phi = (e)$.

To prove that ϕ is an isomorphism of G into $\bar{G}$.

It is enough to prove that ϕ is 1-1.

If $x, y \in G$ then

$\phi(x) = \phi(y) \Rightarrow \phi(x)\phi(y)^{-1} = \phi(y)\phi(y)^{-1}$

$\Rightarrow \phi(x)\phi(y) = \bar{e} \Rightarrow \phi(xy^{-1}) = \bar{e}$

$\Rightarrow xy^{-1} \in k \Rightarrow xy^{-1} \in e \quad [\because k_\phi = (e)]$

$\Rightarrow (xy^{-1})y = e.y$

$\Rightarrow x = y$

$\therefore \phi$ is 1-1.

Hence ϕ is an isomorphism of G into $\bar{G}$.

Fundamental theorem on homomorphism of group:

Theorem:

Let ϕ be a homomorphism of G onto $\bar{G}$ with Kernel k. Then $G/k \cong \bar{G}$.

Proof:

Let us defined the mapping.

$\psi : G/k \to \bar{G}$ is defined by.

$\psi(x) = \phi(g)$ for any $x \in G/k$, $x = kg \quad \forall g \in G$.

we shall prove that $G/k \cong \bar{G}$.

If $g \in G$, then $kg \in G/k$ and $\phi(g) \in \bar{G}$

consider the mapping.

$\psi : G/k \to \bar{G}$ ∋ $\psi(kg) = \phi(g) \quad \forall g \in G$

First we shall show that the mapping ψ is well defined.

We have to Prove that for any $g, g' \in G$ and $kg = kg'$ then $\phi(g) = \phi(g')$

(or) $\varphi(kg) = \varphi(kg')$

$kg = kg'$ then $g = kg'$ where $K \in k$,

$\Rightarrow \phi(g) = \phi(kg')$

$\Rightarrow \phi(g) = \phi(k)\,\phi(g')$

$\Rightarrow \phi(g) = \bar{e}\,\phi(g') \Rightarrow \phi(g) = \phi(g')$

$\Rightarrow \varphi(kg) = \varphi(kg')$

$\therefore \varphi$ is well defined.

φ is onto.

If $\bar{x} \in \bar{G}$, $\bar{x} = \phi(g)$, $g \in G$

so $\bar{x} = \phi(g) = \varphi(kg) = \varphi(x)$.

$\therefore \varphi$ is onto

φ is homomorphism.

If $x, y \in G/k$, $x = kg$, $y = kf$, $g, f \in G$.

$xy = kgkf = kgf$

$\varphi(xy) = \varphi(kgf) = \phi(gf)$

$= \phi(g)\,\phi(f)$ [$\because \phi$ is homomorphism]

$= \varphi(kg)\varphi(kf)$

$= \varphi(x)\varphi(y)$

i.e $\varphi(xy) = \varphi(x)\varphi(y)$

$\therefore \varphi$ is homomorphism.

ψ is 1-1

We have $\psi(Kg) = \psi(Kg')$

$\Rightarrow \phi(g) = \phi(g')$

$\Rightarrow \phi(g)\phi(g')^{-1} = \phi(g')\phi(g')^{-1}$

$\Rightarrow \phi(g)\phi(g')^{-1} = \bar{e}$

$\Rightarrow \phi(g)\phi(g'^{-1}) = \bar{e} \Rightarrow \phi(gg'^{-1}) = \bar{e}$

$\Rightarrow gg'^{-1} \in K \Rightarrow Kg = Kg'$

$\therefore \psi$ is 1-1

Hence $G/K \cong \bar{G}$.

Lemma 2.7.5:

Let ϕ be a homomorphism of G onto $\bar{G}$ with kernel K. For $\hat{H}$ a subgroup of $\bar{G}$. Let H be defined by $H = \{x \in G \mid \phi(x) \in \hat{H}\}$ Then H is a subgroup of G and $H \supset K$; if $\hat{H}$ is normal in $\bar{G}$, then H is normal in G. Moreover, this association sets up a one-to-one mapping from the set of all subgroups of $\bar{G}$ onto the set of all subgroups of G which contain K.

Proof:

Suppose ϕ is a homomorphism of G onto $\bar{G}$ with kernel K, and suppose that $\hat{H}$ is a subgroup of $\bar{G}$.

Let $H = \{x \in G \mid \phi(x) \in \hat{H}\}$.

Now, we prove that H is a subgroup of G and $H \supset K$.

That $H \supset K$ is trivial.

For, if $x \in K$, $\phi(x) = \bar{e}$ is in $\hat{H}$

So, $K \subset H$

Suppose now that $x, y \in H$; hence $\phi(x) \in \hat{H}$, $\phi(y) \in \hat{H}$

$\Rightarrow \phi(xy) = \phi(x).\phi(y) \in \hat{H}$. [$\because \hat{H}$ is a subgroup].

$\therefore xy \in H$

$\therefore H$ is closed under the product in G.

If $x \in H$, $\phi(x) \in \hat{H}$

$\Rightarrow \phi(x)^{-1} \in \hat{H}$ [$\because \hat{H}$ is a subgroup]

$\Rightarrow \phi(x^{-1}) = \phi(x)^{-1} \in \hat{H}$

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

$\therefore H$ is a subgroup of G.

Next we prove that H is normal subgroup of G.

Let $g \in G$, $n \in H$, then $\phi(n) \in \hat{H}$

Let us take $\phi(gng^{-1}) = \phi(g)\,\phi(n)\,\phi(g^{-1})$

$= \phi(g)\,\phi(n)\,\phi(g)^{-1} \in \hat{H}$ [$\because \hat{H}$ is a normal in $\bar{G}$]

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

$\therefore H$ is normal in G.

If ϕ is a homomorphism of G onto $\bar{G}$, we shall considered on elements of H, induces a homomorphism

of H onto $\hat{H}$ with kernel K and also $K \subset H$.

By using the above theorem

$$\hat{H} \cong H/K.$$

Suppose conversely, that L is a subgroup of G. and $K \subset L$.

Let $\bar{I} = \{ \bar{x} \in \bar{G} / \bar{x} = \phi(l), l \in L \}$.

Now we prove that $\bar{I}$ is a subgroup of $\bar{G}$.

Let $\phi(l_1), \phi(l_2)$ be an element of $\bar{I}$ and $l_1, l_2 \in L$.

Now, $l_1, l_2 \in L \Rightarrow l_1 l_2^{-1} \in L$. [$\because$ L is a subgroup of G].

$\Rightarrow \phi(l_1 l_2^{-1}) \in \bar{I}$

$\Rightarrow \phi(l_1)\phi(l_2^{-1}) \in \bar{I}$

$\Rightarrow \phi(l_1)\phi(l_2)^{-1} \in \bar{I}$

$\therefore \bar{I}$ is a subgroup of $\bar{G}$.

Now, let $T = \{ y \in G / \phi(y) \in \bar{I} \}$ is a subgroup of G containing K.

We claim that $L = T$.

Obviously $L \subset T$, since $l \in L \Rightarrow \phi(l) \in \bar{I}$

$\Rightarrow l \in T \rightarrow (1)$

Now to show that $\bar{T} \subset L$

Let $t \in T$, then $\phi(t) \in \bar{I}$ [by definition]

Let $\phi(t) = \phi(l)$ for some $l \in L$

$\Rightarrow \phi(t)\phi(l)^{-1} = \phi(t)\phi(l)^{-1}$

$\Rightarrow \phi(t)\phi(l)^{-1} = \bar{e}$

$\Rightarrow \phi(t)\phi(l^{-1}) = \bar{e}$

$\Rightarrow \phi(tl^{-1}) = \bar{e} \Rightarrow tl^{-1} \in K \subset L$

Thus $t \in Ll = L. \Rightarrow t \in L$

$\therefore T \subset L \rightarrow (2)$

combine (1) & (2) we get

$L = T$

Thus we have set up a one-to-one correspondence between the set of all subgroup of $\bar{G}$ and the set of all subgroup of G which contain K.

Theorem : 2.72.

Let ϕ be a homomorphism of G onto $\bar{G}$ with kernel K, and let $\bar{N}$ be a normal subgroup of $\bar{G}$, $N = \{x \in G / \phi(x) \in \bar{N}\}$. Then $G/N \cong \bar{G}/N$. Equivalently, $G/N \cong (G/K)/(N/K)$.

Proof:

Let θ is a homomorphism of $\bar{G}$ onto $\bar{G}/\bar{N}$ i.e $\theta : \bar{G} \rightarrow \bar{G}/\bar{N}$ is defined by

$\theta(\bar{g}) = \bar{N}\bar{g}$

we define the mapping $\psi : G \rightarrow \bar{G}/\bar{N}$ is

defined by $\psi(g) = \bar{N}\phi(g)$ for all $g \in G$. We shall show that ψ is a homomorphism of G onto $\bar{G}/\bar{N}$ with kernel N.

ψ is onto:

Let $\bar{N}\bar{g} \in \bar{G}/\bar{N}$. Then $\bar{g} \in \bar{G}$

Therefore $\exists\, g \in G \ni \phi(g) = \bar{g}$ [$\because \phi$ is onto]

Now $\psi(g) = \bar{N}\phi(g) = \bar{N}\bar{g}$

$\therefore \psi$ is onto.

ψ is homomorphism:

Let $a, b \in G$ Then $\psi(ab) = \bar{N}\phi(ab)$

$\psi(ab) = \bar{N}\phi(a,b)$

$= \bar{N}\phi(a)\phi(b)$ [$\because \phi$ is homomorphism]

$= [\bar{N}\phi(a)][\bar{N}\phi(b)]$

$\psi(ab) = \psi(a).\psi(b).$

$\therefore \psi$ is a homomorphism of G onto $\bar{G}/\bar{N}$

Now to show that Kernel of ψ is N.

Suppose that we take the Kernel of ψ is T.

If $n \in N$, $\phi(n) \in \bar{N}$

So that $\psi(n) = \bar{N}\phi(n)$

$\psi(n) = \bar{N}$ [$\because \phi(n) \in N$]

$\Rightarrow$ The Identity element of $\bar{G}/\bar{N}$

$\Rightarrow n \in T$ $\quad N \subset T \rightarrow$ (I)

on the otherhand, if $t \in T$

$\Rightarrow \psi(t)$ = identity element of $\bar{G}/\bar{N}$

$\psi(t) = \bar{N} \rightarrow (1)$

But $\psi(t) = \bar{N}\phi(t) \rightarrow (2)$

comparing (1) & (2) we get

$\bar{N} = \bar{N}\phi(t)$

$\Rightarrow \phi(t) \in \bar{N} \Rightarrow t \in N$ [By definition of $\bar{N}$]

$\therefore T \subset N \rightarrow$ (II)

From I & II

$T = N$

i,e the kernel of ψ will be equal to N.

$\therefore \psi$ is a homomorphism of G onto $\bar{G}/\bar{N}$ with kernel N

By using Fundemental theorem of homomorphism.

we get $G/N \cong \bar{G}/\bar{N}$

By using the above same theorem we get

$\bar{G} \cong G/K$, $\bar{N} \cong N/K$, $\bar{G}/\bar{N} \cong (G/K)/N/K$

Thus $G/N \cong (G/K)/(N/K)$

[$G/N \cong \bar{G}/\bar{N} \cong (G/K)/(N/K)$

Since $\bar{G} \cong G/K$, $\bar{N} \cong N/K$].