which of the following sets are subspace of V_3

Group Theory

Def^n. - (Group)

A non-empty set of elements G is said to form a group if in G there is defined a binary operation, called the Product and denoted by (.) s.t

(1) $a, b \in G \Rightarrow a \cdot b \in G$ (Closure law)

(2) $a, b, c \in G \Rightarrow a\cdot(b\cdot c) = (a\cdot b)\cdot c$ (Associative law)

(3) There exist an element $e \in G$ s.t $a \cdot e = ea = a$ for all $a \in G$ (Existence of an identity element in G)

4. For every $a \in G$ $\exists$ an $a^{-1} \in G$ s.t

$$a \cdot a^{-1} = a^{-1} \cdot a = e$$

Abelian or Commutative Group

A group G is said to be abelian group if for every $a, b \in G$, $a \cdot b = b \cdot a$

Order of a group :— The number of elements present in a group is called the order of the group. It is denoted by $o(G)$. If the order is finite. Then it is said to be finite group.

Semi - group :- A non-empty set G is said to be a semigroup under the binary operation if it satisfies the associative property.

Lemma- 2.3.1

If G is a group then

(a) The identity element of G is unique.

(b) Every $a \in G$ has a unique inverse in G

(c) For every $a \in G$ $(a^{-1})^{-1} = a$

(d) For every $a.b \in G$ $(a \cdot b)^{-1} = b^{-1} a^{-1}$

Proof

(a) To prove that the identity element of group G is unique.

Assume that the identity element of G is not unique.

$\Rightarrow \exists$ atleast two different identity elements in G.

Let e and f be two different identity elements in G.

e is an identity element of G.

$\Rightarrow a \cdot e = e \cdot a = a \quad \forall a \in G$.

In particular for $f \in G$

$f \cdot e = e \cdot f = f$ — (1)

Again f is an identity element of G

$\Rightarrow a \cdot f = f \cdot a = a \quad \forall a \in G$.

In particular for $e \in G$

$e \cdot f = f \cdot e = e$ — (2)

Now $e = f \cdot e$
$= f$

$e = f$

This contradicts to the fact that e and f are different.
Therefore the identity element of G is unique.

Proof-(b)

To prove that a has a unique inverse in G.

Assume that a has not unique inverse in G,
$\Rightarrow \exists$ at least two different inverse element of a.
Let x and y be two different inverse elements of a
x is an inverse element of a
$\Rightarrow x \cdot a = a \cdot x = e$
Also y is an inverse element of a
$\Rightarrow y \cdot a = a \cdot y = e$

Now $x = x \cdot e$ (Existence of identity element in G)
$= x (a \cdot y)$
$= (x \cdot a) y$ (By associative law)
$= e \cdot y$
$= y$
$\Rightarrow x = y$

This contradicts to the fact that x and y are different.
So a has a unique inverse in G.
Since a in G is arbitrary.
So, every a in G has a unique inverse in G.

Proof-(C)

To prove that $(a^{-1})^{-1} = a \ \forall a \in G$

let $a \in G$ be arbitrary,

To show that $(a^{-1})^{-1} = a$.

$a \in G \Rightarrow \exists a^{-1}$ in G s.t

$a \cdot a^{-1} = a^{-1} a = e$ — (1) (existence of inverse element in G)

Now $a^{-1} \in G \Rightarrow \exists (a^{-1})^{-1}$ in G s.t

$a^{-1}(a^{-1})^{-1} = (a^{-1})^{-1} \cdot a^{-1} = e$.

Now $a = a \cdot e$

$= a \cdot \{a^{-1}(a^{-1})^{-1}\}$

$= \{a \cdot a^{-1}\} \cdot (a^{-1})^{-1}$, by associative law

$= e \cdot (a^{-1})^{-1}$

$= (a^{-1})^{-1}$ existence of identity element.

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

Since $a \in G$ be arbitrary,

So for every $a \in G$, $(a^{-1})^{-1} = a$.

So $(a^{-1})^{-1} = a \ \forall a \in G$.

Proof-d

To prove that

$(a \cdot b)^{-1} = b^{-1} a^{-1} \ \forall a, b \in G$,

Let $a, b \in G$ be arbitrary,

$(a \cdot b) \cdot (b^{-1} a^{-1}) = C(b^{-1} a^{-1})$ [Take $C = a \cdot b$]

$= (C \cdot b^{-1}) a^{-1}$, By associative axiom

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

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

$= (a \cdot e) a^{-1}$ (existence of inverse element in G)

$= a \cdot a^{-1} = e$ (existence of identity element in G)

$\Rightarrow (a \cdot b)(b^{-1} a^{-1}) = e.$

$(b^{-1} a^{-1})(a \cdot b)$

$= (b^{-1} a^{-1}) c$

$= b^{-1}(a^{-1} c)$, Associative Law.

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

$= b^{-1}\{(a^{-1}a)b\}$ By associative Law.

$= b^{-1}(e \cdot b)$ (existence of inverse element in G.)

$= b^{-1} b = e$

So $(ab)(b^{-1}a^{-1}) = (b^{-1}a^{-1})(a \cdot b) = e$

So $b^{-1}a^{-1}$ is the inverse of $(a \cdot b)$

(i.e) $\Rightarrow b^{-1} \cdot a^{-1} = (a \cdot b)^{-1}$

Lemma - 2.3.2

Given a, b in the group G, then the equations $a \cdot x = b$ and $y \cdot a = b$, have unique solutions for x and y in G.

In particular, the two cancellation laws

$a \cdot u = a \cdot w \Rightarrow u = w$

$u \cdot a = w \cdot a \Rightarrow u = w$

hold in G.

Proof

Given that a, b are in the group G.

To show that the equation $a \cdot x = b$ has a unique solution.

We shall prove this by method of contradiction.

Assume that the equation $a \cdot x = b$ has not unique sol^n.

$\Rightarrow \exists$ atleast 2 different sol^n of the equation $a \cdot x = b$.

Let x_1 and x_2 be 2 different solutions of the equation $a \cdot x = b$

$\Rightarrow a \cdot x_1 = b$ and $a \cdot x_2 = b$ — (1)

$\Rightarrow a x_1 = a x_2$

Now, $x_1 = e x_1$ [existence of identity element]

$= (a^{-1} \cdot a) x_1$ (" inverse element)

$= a^{-1} \cdot (a \cdot x_1)$ (associative law

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

$= (a^{-1} a) x_2$ (associative law)

$= e \cdot x_2$, identity element

$= x_2$

$\Rightarrow x_1 = x_2$

This contradicts to the fact that x_1 and x_2 are different.

Therefore $ax = b$ has unique solution.

Next to show that the equation $ya = b$ has a unique sol^n.

Assume $ya = b$ has not unique sol^n,

$\Rightarrow \exists$ atleast two different solⁿ of $ya=b$.

Let y_1 and y_2 be 2 different solⁿ of the eqⁿ $ya=b$.

$\Rightarrow y_1 a = b$ & $y_2 a = b$

$\Rightarrow y_1 a = y_2 a$

Now $y_1 = y_1 e$, existence of identity element

$= y_1 (a \cdot a^{-1})$ inverse element

$= (y_1 a) a^{-1}$, associative law

$= (y_2 a) a^{-1}$

$= y_2 (a a^{-1})$,

$= y_2 \cdot e = y_2$

This contradicts to the fact that y_1 and y_2 are different.

Hence $ya=b$ has a unique solⁿ.

Again, Next to prove that :

(i) $a \cdot u = a \cdot w \Rightarrow u = w$

(ii) $u \cdot a = w \cdot a \Rightarrow u = w$

Proof (i) $a \cdot u = a \cdot w$

$\Rightarrow a \cdot u = a \cdot w = b$

$\Rightarrow a \cdot u = b$ and $a \cdot w = b$

$\Rightarrow u$ and w are solⁿ of eqⁿ. $ax = b$

$\Rightarrow u = w$ [$\because$ The eqⁿ $ax = b$ has a unique solⁿ.

(ii) $u \cdot a = w \cdot a$

$\Rightarrow u a = w \cdot a = b$

$\Rightarrow u \cdot a = b$ & $w \cdot a = b$

$\Rightarrow u$ and w are solⁿ of eqⁿ $ya=b$

$\Rightarrow u = \omega$. ($\because$ The equation $ya=b$ has a unique sol

Problems.

Q-2 Proof

G is an abelian group

To show that $(a \cdot b)^n = a^n \cdot b^n \quad \forall\, a, b \in G$ and $n \in Z^+$

We shall prove this by method of inducti

let $P_n \equiv (a \cdot b)^n = a^n \cdot b^n \quad \forall\, a \cdot b \in G$

First to show that P_1 is true

i.e to show that $(a \cdot b)^1 = a^1 b^1$.

L.H.S $(a \cdot b)^1 = ab$

~~Assume~~ R.H.S $a^1 \cdot b^1 = ab$, L.H.S = R.H.S

Assume P_k is true.

i.e $(a \cdot b)^k = a^k \cdot b^k$

To show that P_{k+1} is true.

i.e to show that $(a \cdot b)^{k+1} = a^{k+1} \cdot b^{k+1}$

L.H.S $(a \cdot b)^{k+1}$

$= (a \cdot b)(a \cdot b)^k$

$= (a \cdot b)(a^k \cdot b^k)$ by assumption.

$= \{(a \cdot b) a^k\} b^k$ $\because$ by associative law.

$\Rightarrow a \cdot a^k b$

$= \{a \cdot (b \cdot a^k)\} b^k$

$= \{a \cdot (a^k \cdot b)\} b^k$, $\because$ G is abelian

$= \{(a \cdot a^k)(b b^k)\}$

$= \{(a \cdot a^k) b\} b^k$

$= (a \cdot a^k)(b b^1)$

$= a^{k+1} \cdot b^{k+1}$

P_{k+1} is true

Hence by method of induction P_n is true for +ve integers n.

(6) If G is a group s.t $(a \cdot b)^2 = a^2 \cdot b^2$ for all $a, b \in G$. Show that G must be abelian.

Proof

Given that $(a \cdot b)^2 = a^2 b^2 \; \forall \; a, b \in G$.

To show that G is abelian

we have $(a \cdot b)^2 = a^2 \cdot b^2 \quad \forall \; a \cdot b \in G$

$\Rightarrow (a \cdot b)(a \cdot b) = a \cdot a \cdot b \cdot b$

$\Rightarrow \{(a \cdot b) \cdot a\} \cdot b = a \cdot a \cdot b \cdot b \; \forall \; a, b \in G$

$\Rightarrow (a \cdot b) a = a \cdot a \cdot b \quad \forall a, b \in G$. (By right cancellation Law for multiplication.

$\Rightarrow a \cdot (b \cdot a) = a \cdot a \cdot b \; \forall \; a, b \in G$. (associative law)

$\Rightarrow b \cdot a = a \cdot b$

$\Rightarrow G$ is abelian.

PROOF

18. Given that every element of the group G is its own inverse.

To show that G is abelian.

i.e to show that $a \cdot b = b \cdot a$ $\forall a, b \in G$

let $a, b \in G$ be arbitrary.

$\Rightarrow ab \in G$ (closure axiom)

So $a = a^{-1}, b = b^{-1}$

and $(ab) = (ab)^{-1}$ [Every element of the group G its own inverse

Now $ab = (ab)^{-1}$

$\Rightarrow ab = b^{-1} a^{-1}$

$\Rightarrow ab = ba$ ($\because b^{-1} = b$ and $a^{-1} = a$)

Since $a, b \in G$ are arbitrary

So $ab = ba$ $\forall a, b \in G$

Hence G is abelian.

2.4 Subgroups (1)

Def^n:- A non empty subset H of a group G is said to be a subgroup of G if H itself forms a group under the same binary operation as defined in G.

Lemma - 2.4.1

A nonempty subset H of the group G is a subgroup of G if and only if

1. $a, b \in H \Rightarrow ab \in H$
2. $a \in H \Rightarrow a^{-1} \in H$.

Proof

Given that H is a non-empty subset of the group G.

Also H is a subgroup of G.

To show that

1. $a, b \in H \Rightarrow ab \in H$
2. $a \in H \Rightarrow a^{-1} \in H$

We have given that H is a subgroup of G.

$\Rightarrow H$ forms a group (By def^n of subgroup)

$\Rightarrow$ All the four group axioms are satisfied in H.

$\Rightarrow$ 1. $a, b \in H \Rightarrow ab \in H$

and 2. $a \in H \Rightarrow a^{-1} \in H$

Conversely

Given that H is a nonempty subset of the group G.

Also $a, b \in H \Rightarrow ab \in H$ and $a \in H \Rightarrow a^{-1} \in H$.

To show that H is a subgroup of G i.e to prove that

(i) $a, b, c \in H \Rightarrow a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(ii) $\exists$ an element $e \in H$ s.t $a \cdot e = e \cdot a = a \ \forall a \in H$.

(i) $a, b, c \in H$

$\Rightarrow a, b, c \in G$ $\quad (\because H \subseteq G)$

$\Rightarrow a\cdot(b\cdot c) = (a\cdot b)\cdot c$ $\left\{ \begin{array}{l} \text{associative axiom} \\ \text{is satisfied in } G \end{array} \right\}$

So $a, b, c \in H \Rightarrow a\cdot(b\cdot c) = (a\cdot b)\cdot c$

(ii) To prove that $\exists$ an element e in H s.t

$$a\cdot e = e\cdot a = a \quad \forall a \in H$$

Let $a \in H$ be arbitrary

First to show that $e \in H$

we have $a \in H$

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

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

$\Rightarrow e \in H$

So $e \in H$

Now $a \in H \Rightarrow a \in G$ $\quad (\because H \subseteq G)$

$\Rightarrow a\cdot e = e\cdot a = a$

$\exists$ an element e in H, s.t $a\cdot e = e\cdot a = a$, where $a \in H$

Since $a \in H$ is arbitrary,

So $\exists$ an element e in H s.t

$a\cdot e = e\cdot a = a \quad \forall a \in H$.

Lemma 2.4.2

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

Proof

Given that H is a nonempty finite subset of a group G.

Also H is closed under multiplication.

To show that H is a subgroup of G.

i.e to prove that

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

$a \in H$

$\Rightarrow a.a \in H$ ($\because$ H is closed under multiplication)

$\Rightarrow a^2 \in H.$

Again $a^2 \in H$, $a \in H$

$\Rightarrow a^2 a \in H$

$\Rightarrow a^3 \in H$.

Similarly $a^4, a^5 \ldots\ldots$ are all in H.

Thus the infinite collection of elements $a, a^2, a^3 \ldots\ldots$ must all fit into H.

But H is given to be finite.

So there must be repetition in this collection of elements.

Let $a^r = a^s$ where r and s are +ve integers with $r > s$

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

$\Rightarrow e \in H$. ($\because$ r-s is a +ve integer, So $a^{r-s} \in H$)

we have

r and s are +ve integers with $r > s$.

$\Rightarrow r-s-1 \geq 0$

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

$\Rightarrow a^{r-s} . a^{-1} \in H \Rightarrow e.a^{-1} \in H$

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

Hence H is a subgroup of G.

Defn. :- Let H be a subgroup of a group G. Let $a, b \in G$, a is congruent to b modulo H is denoted by $a \equiv b \bmod H$ and is defined by $a \equiv b \bmod H \Leftrightarrow ab^{-1} \in H$.

Lemma - 2.4.3

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

Proof

To prove that the relation $a \equiv b \bmod H$ is an equivalence relation.

i.e to show that
The relation $a \equiv b \bmod H$ is reflexive, symmetric and transitive

i.e to prove that
1. $a \equiv a \bmod H$ .. is reflexive
2. $a \equiv b \bmod H \Rightarrow b \equiv a \bmod H$
3. $a \equiv b \bmod H$ and $b \equiv c \bmod H \Rightarrow a \equiv c \bmod H$

1. clearly $e \in H$ ($\because$ H is a subgroup of G)

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

$\Rightarrow a \equiv a \bmod H$

(2) $a \equiv b \bmod H$

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

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

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

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

$\Rightarrow b \equiv a \bmod H$

(3) $a \equiv b \bmod H$, and $b \equiv c \bmod H$

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

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

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

$\Rightarrow a \equiv c \bmod H$

Hence the relation $a \equiv b \bmod H$ is reflexive Symmetric and transitive.
So $a \equiv b \bmod H$ is an equivalence relation.

Defⁿ:- If H is a subgroup of a group G and $a \in G$.

$Ha = \{ha \mid h \in H\}$ Ha is called a right coset of H in G

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

aH is called a left coset of H in G.

Lemma - 2.4.4

For all $a \in G$.

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

Proof

To show that $Ha = \{x \in G \mid a \equiv x \bmod H\}$

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

To show that $Ha = [a]$

let $x \in Ha$

$\Rightarrow x = ha$ where $h \in H$

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

$\Rightarrow xa^{-1} = h(aa^{-1})$ associative law

$\Rightarrow xa^{-1} = he$ existence of inverse element in G.

$\Rightarrow xa^{-1} = h$ existence of identity element in G.

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

$x \equiv a \bmod H$

$\Rightarrow a \equiv x \bmod H$ ($\because$ congruency modulo relation is symmetric)

1

$\Rightarrow x \in [a]$

So $x \in Ha \Rightarrow x \in [a]$

Hence $Ha \subseteq [a]$ ——— (1)

Let $x \in [a]$

$\Rightarrow a \equiv x \bmod H$

$\Rightarrow x \equiv a \bmod H$

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

$\Rightarrow (x \cdot a^{-1}) \cdot a \in Ha$

$\Rightarrow x (a^{-1} a) \in Ha$ associative

$\Rightarrow x e \in Ha$

$\Rightarrow x \in Ha$

$\Rightarrow x \in [a]$

Hence $\Rightarrow x \in Ha$

$[a] \subseteq Ha$ ——— (2)

From (1) and (2)

$Ha = [a]$

Lemma - 2.4.5

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

Proof

To prove that there is a one-to-one correspondence between any two right cosets of H in G,

Let Ha, Hb be any two right cosets of H in G.

Claim :- To prove that there is a one-to-one correspondence between Ha and Hb.

Let $f: Ha \to Hb$ be defined by

$f(ha) = hb \quad \forall \ ha \in Ha$

First to show that $f: Ha \to Hb$ is one-one

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

$\Rightarrow h_1 b = h_2 b$

$\Rightarrow h_1 = h_2$

$\Rightarrow h_1 a = h_2 a$

Hence $f(h_1 a) = f(h_2 a) \Rightarrow h_1 a = h_2 a$

Hence $f: Ha \to Hb$ is one-one.

Next to show that $f: Ha \to Hb$ is onto.

i.e to show that for every y in Hb $\exists$ atleast one x in $H.a$ $\to x \in Ha$ s.t $y = f(x)$.

Let y in Hb be arbitrary.

$\Rightarrow y \in Hb$

$\Rightarrow y = hb$, where $h \in H$

Now $h \in H \Rightarrow ha \in Ha$

$\Rightarrow x \in Ha$ (Taking $ha = x$)

By defn of f,

$f(ha) = hb$

$\Rightarrow f(x) = y$

So, for y in Hb, $\exists$ x in Ha s.t $y = f(x)$.

Since y in Hb is arbitrary.

So for every y in Hb

$\exists$ x in Ha s.t $y = f(x)$.

Hence $f: Ha \to Hb$ is onto.

$\therefore f: Ha \to Hb$ is one-one and onto.

$\Rightarrow \exists$ a one-to-one correspondence between Ha and Hb.

Since Ha and Hb are any two right cosets of H in G.

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

Th - 2.4.1 (Lagrange's Th.) 16 9-4a

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

Proof

We know that congruence mod(H) on G is an equivalence relation. The right cosets of H in G are equivalence classes.

An equivalence relation on G decomposes it as union of disjoint equivalence classes.

Since G is finite, the relation congruence mod(H) decomposes G as union of finite number (let n) of equivalence classes.

$$\text{So } G = \bigcup_{i=1}^{n} Ha_i$$

where $Ha_i \cap Ha_j = \phi$ for $i \neq j$.

$$\Rightarrow O(G) = O\left(\bigcup_{i=1}^{n} Ha_i\right)$$

$$= \sum_{i=1}^{n} O(Ha_i)$$

But $\exists$ 1-1 correspondence between any two right cosets of H in G and $H = He$ is an right coset.

Hence $O(Ha_i) = O(H)$ $\forall i$

$$O(G) = \sum_{i=1}^{n} O(Ha_i) = \sum_{i=1}^{n} O(H) = n\,O(H)$$

$$\therefore O(H) \mid O(G)$$

Def^n:- If H is a subgroup of G, the index of H in G is the number of distinct right cosets of H in G.

Def^n:- If G is a group and $a \in G$, the order of a is the least positive integer m s.t $a^m = e$.

Corollary:

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

Proof

Given that G is a finite group and $a \in G$.

To prove that $o(a) | o(G)$

Let H be the cyclic subgroup of G generated by a.

i.e $H = \{a^i \mid i = 0, \pm1, \pm2 \dots\}$

Claim: To prove that H contain exactly $o(a)$ number of elements.

First to show that H can not contain more than $o(a)$ number of elements

we know that $a^{o(a)} = e$

$\Rightarrow$ H cannot contain more than $o(a)$ number of elements

[$\because$ in H every term is repeated after $o(a)$ number of elements]

Next, to show that H can not contains less than $o(a)$ number of elements

If possible some elements in the collection $a^0 = e, a^1, a^2 \dots a^{o(a)-1}$ could be repeated.

Let $a^i = a^j$, where $0 \le i < j < o(a)$

$\Rightarrow a^{j-i} = e$

Now $0 \le i < j < o(a)$

$\Rightarrow j-i > 0$ and $j-i < o(a)$

$\Rightarrow j-i$ is a +ve integer less than $o(a)$

So $j-i$ is a +ve integer less than $o(a)$ and $a^{j-i} = e$.

This contradicts to the fact that $o(a)$ is the least +ve integer s.t $a^{o(a)} = e$.

Hence H cannot contain $o(a)$ number of elements. Therefore H contains exactly $o(a)$ number of elements.

So $o(H) = o(a)$

Now H is a subgroup of a finite group G.

$\Rightarrow o(H) \mid o(G)$ (By Lagrange's Th.)

$\Rightarrow o(a) \mid o(G)$

Corollary-2

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

Proof

Given that G is finite group and $a \in G$

To show that $a^{o(G)} = e$

Since G is a finite group and $a \in G$

So $o(a) \mid o(G)$

$\Rightarrow o(G) = k\, o(a)$, k is an integer

Now $a^{o(G)} = a^{k\,o(a)} = \{a^{o(a)}\}^{k} = (e)^{k} = e$

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

Corollary - 3 (Euler's Thm)

Euler's ϕ function:-

Let n be a positive integer,

if $n=1$, then $\phi(n) = 1$

if $n>1$, then $\phi(n)$ is the number positive integers less than n and relatively prime to n

if p is a prime number, then $\phi(p) = p-1$.

Corollary - 3 (Euler)

if n is a positive integer and a is relatively prime to n, then $a^{\phi(n)} \equiv 1 \bmod n$.

Proof

Given that n is a positive integer and a is relatively prime to n

To prove that $a^{\phi(n)} \equiv 1 \bmod n$

We know that G is the set of +ve integers less than n and relatively prime to n.

then G is a group under multiplication modulo n. and $o(G) = \phi(n)$

Case-1 if $a < n$

Now a is a +ve integer less than n and relatively prime to n.

$\Rightarrow a \in G$ (By $\overset{(2)}{\text{Lagrange's theorem}}$)

$\Rightarrow a^{O(G)} = 1$ $\quad [\because O(G) = \phi(n)]$

$\Rightarrow a^{\phi(n)} = 1$

$\Rightarrow a^{\phi(n)} - 1 = 0$

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

$\Rightarrow a^{\phi(n)} \equiv 1 \bmod n.$

Case-2: If $a > n$

$a > n \Rightarrow \exists$ an integer m and r s.t. $a = mn + r$ where $0 < r < n$

$\Rightarrow a = mn + r$

$\Rightarrow a - r = mn$

$\Rightarrow n \mid (a - r)$

$\Rightarrow n \mid (a^{\phi(n)} - r^{\phi(n)})$

$\Rightarrow a^{\phi(n)} \equiv r^{\phi(n)} \bmod (n)$ ——— (1)

Now r is a +ve integer less than n and relatively prime to n

$\Rightarrow r \in G$

$\Rightarrow r^{O(G)} = 1$

$\Rightarrow r^{\phi(n)} = 1$

$\Rightarrow r^{\phi(n)} - 1 = 0$

$\Rightarrow n \mid r^{\phi(n)} - 1$

$\Rightarrow r^{\phi(n)} \equiv 1 \bmod n.$ ——— (2)

From ① and ② we get

$$a^{\phi(m)} \equiv 1 \bmod m$$

From case-I and II we conclude that

$$a^{\phi(m)} \equiv 1 \bmod m.$$

Corollary-4 (Fermat)

If P is a prime number and a is any integer, then $a^P \equiv a \bmod P$.

Proof

P is a prime number and a is any integer.

To prove that $a^P \equiv a \bmod P$

Since P is a prime number

So $\phi(P) = P-1$

Case-1

If a is relatively prime to P and a is relatively prime to P.

$\Rightarrow a^{\phi(P)} \equiv 1 \bmod P$, by euler th.

$\Rightarrow a^{P-1} \equiv 1 \bmod P$

$\Rightarrow P \mid a^{P-1}-1$

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

$\Rightarrow P \mid a^P - a$

$\Rightarrow a^P \equiv a \bmod P$

Case-2

If a is not relatively prime to P. Since P is prime.

So $p \mid a$

$\Rightarrow p \mid a \cdot a^{p-1}$

$\Rightarrow p \mid (a^p - 0)$

$\Rightarrow a^p \equiv 0 \bmod p$

Again $p \mid a$

$\Rightarrow p \mid (a-0)$

$\Rightarrow a \equiv 0 \bmod p$

$\Rightarrow a \equiv 0 \bmod p$

$\therefore a^p \equiv a \bmod p$

From Case-I and II we conclude that

$a^p \equiv a \bmod p$

Corollary-5

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

Proof

Given that G is a finite group whose order is a prime number p.

To prove that G is a cyclic group.

we have given that

$o(G) = p$, where p is a prime number

$\Rightarrow o(G) > 1$

$\exists$ atleast one element 'a' in G

s.t $a \neq e$,

Let H be the cyclic subgroup of G generated by a

i.e $H = \{a^i \mid i = 0, \pm1, \pm2, \cdots\} = (a)$

Now, H is a subgroup of a finite group G,

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

$\Rightarrow o(H) \mid p$

$\Rightarrow o(H) = 1$ or $o(H) = p$ $(\because p$ is prime$)$

$\Rightarrow H = \{e\}$ or $o(H) = o(G)$ $(\because p = o(G))$

$\Rightarrow H = \{e\}$ or $H = G$.

$\Rightarrow H = G$. $(\because a \neq e$ is in $H)$

$\Rightarrow G = (a)$ $\{\because H = (a)\}$

$\Rightarrow$ G is a cyclic group.

2.5 A Counting Principle.

Let H and K be subgroups of a group G. Then their multiplication is a set denoted by HK and is defined by

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

Lemma - 2.5.1

HK is a subgroup of G if and only if HK = KH

Proof ($\Rightarrow$)

Given that HK is a subgroup of G

To prove that HK = KH

let $x \in HK$

$\Rightarrow x^{-1} \in HK$ [$\because HK$ is a subgroup of G]

$\Rightarrow x^{-1} = hk$ where $h \in H$, $k \in K$

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

$\Rightarrow x = k^{-1}h^{-1}$ [$\because (ab)^{-1} = b^{-1}a^{-1}$]

$\Rightarrow x \in KH$ $\quad k^{-1} \in K,\ h^{-1} \in H.$

So $HK \subseteq KH$ ——— (1)

let $x \in KH$

$\Rightarrow x = k_1 h_1$ $\quad k_1 \in K,\ h_1 \in H$

$\Rightarrow x^{-1} = (k_1 h_1)^{-1}$

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

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

$\Rightarrow (x^{-1}) \in HK$ [$\because HK$ is a subgroup of G, $(a^{-1})^{-1} = a$]

$\Rightarrow (x^{-1})^{-1} \in HK$ [$\because HK$ is a subgroup of G, $(a^{-1})^{-1} = a$]

$\Rightarrow x \in HK$

So $KH \subseteq HK$ ——— (2)

From (1) and (2)

$HK = KH$

Conversely $HK = KH$

To prove that HK is a subgroup of G.

i.e to prove that

(i) HK is a nonempty subset of G

(ii) $x, y \in HK \Rightarrow xy \in HK$

(iii) $x \in HK \Rightarrow x^{-1} \in HK$

To prove that HK is a non-empty subgroup of G clearly,

$e \in H,\ e \in K$ [∵ H & K are subgroup of G]

$\Rightarrow e \cdot e \in HK$

$\Rightarrow e \in HK$

$\Rightarrow$ HK is nonempty

(i) let $x \in HK$

$\Rightarrow x = hk$, where $h \in H,\ k \in K$

Now $h \in H,\ k \in K$. $(\because H \subseteq G,\ K \subseteq G)$

$\Rightarrow h \in G,\ k \in G$

$\Rightarrow hk \in G$ to closure law is satisfied

$\Rightarrow x \in G$

$\Rightarrow HK \subseteq G$

So HK is a non-empty subset of G

(ii) To prove that $x, y \in H \Rightarrow xy \in HK$

$x, y \in HK$

$\Rightarrow x = h_1 k_1,\ y = h_2, k_2$

$\Rightarrow xy = (h_1 k_1)(h_2 k_2)$

$xy = h_1\{k_1 (h_2 k_2)\}$

$\Rightarrow xy = h_1\{(k_1 h_2) k_2\}$, associative

$\Rightarrow xy = h_1\{(h_3 k_3) k_2\}$ [∵ $h_1 h_2 \in KH$ $\Rightarrow k_1 h_2 \in HK$ as $HK = KH$ $\Rightarrow k_1 h_2 = h_3 k_3$ where $h_3 \in H$, $k_3 \in K$]

associative

$\Rightarrow xy = h_1\{h_3(k_3k_2)\}$

$\Rightarrow xy = (h_1h_3)(k_3k_2)$

$\Rightarrow xy \in HK$

(iii) To prove that $x \in HK \Rightarrow x^{-1} \in HK$.

Let $x \in HK$.

$\Rightarrow x = h_1k_1$ where $h_1 \in H$, $k_1 \in K$

$\Rightarrow x^{-1} = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1}$

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

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

Hence HK is a subgroup of G.

Corollary

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

Proof

Given that H, K are subgroups of an abelian group G.

To prove that HK is a subgroup of G

i.e. to prove that $HK = KH$

let $x \in HK$

$\Rightarrow x = hk$ where $h \in H, k \in K$

$\Rightarrow x = kh$ $\left[\begin{array}{l} \because h \in H,\ k \in K \Rightarrow h \in G,\ k \in G \\ \text{as } H \subseteq G \text{ as } K \subseteq G \\ \Rightarrow hk = kh \text{ as } G \text{ is abelian} \end{array}\right.$

$\Rightarrow x \in KH$

So $HK \subseteq KH$

Next, Let $x \in KH$

$\Rightarrow x = kh$, where $k \in K$, $h \in H$

$\Rightarrow x = hk$

$\Rightarrow k \in G$, $h \in G$ as $H \subseteq G$, $K \subseteq G \Rightarrow kh = hk$, as G is abelian.

$\Rightarrow x \in HK$

So $KH \subseteq HK$

Hence $HK = KH$.

So HK is a subgroup of G.

Th- 2.5.1

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

Given that H and K are finite subgroups of G of orders $o(H)$ and $o(K)$ respectively.

To prove that $o(HK) = \dfrac{o(H)\, o(K)}{o(H \cap K)}$

We have given that H and K are subgroups of G

$\Rightarrow H \cap K$ is a subgroup of G.

$\Rightarrow$ All the four group axioms are satisfied in $H \cap K$

$\Rightarrow H \cap K$ is a subgroup of K $[\because H \cap K \subseteq K$

$\Rightarrow H \cap K$ is a subgroup of a finite group K.

$\Rightarrow o(H \cap K) \mid o(K)$, by Lagrange's Th.

$\Rightarrow \dfrac{o(K)}{o(H \cap K)} = m$, where m is a +ve integer.

$\Rightarrow$ There are m number of distinct right cosets of $H\cap K$ in K.

Let $Dk_1, Dk_2, \ldots, Dk_m$ be m number of distinct right cosets of D in K. [where $D = H\cap K$]

Let $Dk_1, Dk_2 \ldots Dk_m$ be m number of distinct right cosets of D in K.

So $K = (Dk_1 \cup Dk_2 \cup \cdots \cup Dk_m)$

$\Rightarrow HK = H(Dk_1 \cup Dk_2 \cup \cdots \cup Dk_m)$

$\Rightarrow HK = HDk_1 \cup HDk_2 \cup \cdots \cup HDk_m$

$\Rightarrow HK = Hk_1 \cup Hk_2 \cup \cdots \cup Hk_m$ —— (1)

Claim

To prove that $Hk_1, Hk_2, \ldots, Hk_m$ are pairwise disjoint.

If possible

Let $Hk_i = Hk_j$ where $i \neq j$

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

$\Rightarrow k_i k_j^{-1} \in H$ $\quad (\because Ha = H \Leftrightarrow a \in H)$

Again $k_i, k_j \in K$

$\Rightarrow k_i, k_j^{-1} \in K$

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

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

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

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

$\Rightarrow k_i k_j^{-1} \in D$.

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

this contradicts to the fact that

$D_{k_1}, D_{k_2}, \dots D_{k_m}$ are distinct.

Therefore $H_{k_1}, H_{k_2}, \dots H_{k_m}$ are pairwise disjoint.

From (1) we have

$$HK = H_{k_1} \cup H_{k_2} \cup \dots \cup H_{k_m}$$

$$o(HK) = o(H_{k_1} \cup H_{k_2} \cup \dots \cup H_{k_m})$$

$$= o(H_{k_1}) + o(H_{k_2}) + \dots + o(H_{k_m})$$

[$\because H_{k_1}, \dots H_{k_m}$ are pairwise disjoint.

$$= o(H) + o(H) + \dots + o(H) \text{ m times}$$

$$= m\, o(H)$$

$$= \frac{o(K)}{o(D)}\, o(H)$$

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

$$\Rightarrow o(HK) = \frac{o(H)\, o(K)}{o(H \cap K)}$$

Corollary

If H and K are subgroups of G and $o(H) > \sqrt{o(G)}$, $o(K) > \sqrt{o(G)}$, then $H \cap K \neq \{e\}$

Proof

Given that H and K are subgroups of G

and $o(H) > \sqrt{o(G)}$, $o(K) > \sqrt{o(G)}$

To prove that $H \cap K \neq e$

We know that $HK = \{ x \in G / x = hk, h \in H, k \in K \}$

$HK \subseteq G$

$\Rightarrow o(HK) \leq o(G)$

$\Rightarrow \dfrac{o(H)\, o(K)}{o(H \cap K)} \leq o(G)$

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

$\Rightarrow o(G) \geq \dfrac{o(H)\, o(K)}{o(H \cap K)} > \dfrac{\sqrt{o(G)}\,\sqrt{o(G)}}{o(H \cap K)} = \dfrac{o(G)}{o(H \cap K)}$

$\Rightarrow o(G) > \dfrac{o(G)}{o(H \cap K)}$

$\Rightarrow 1 > \dfrac{1}{o(H \cap K)}$

$\Rightarrow o(H \cap K) > 1$

$\Rightarrow H \cap K \neq (e)$

Problems.

1. Given H and K are subgroup of G.

To prove $H \cap K$ is a subgroup of G.

Let $ab \in H \cap K$

$\Rightarrow ab \in H$ and $ab \in K$

$\Rightarrow ab \in H$ and $ab \in K$ [$\because H$ & K are subgroups]

$\Rightarrow ab \in H \cap K$.

Next, let $a \in H \cap K$

$\Rightarrow a \in H$ and $a \in K$

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

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

Hence $H \cap K$ is a subgroup of G.

2. Let G be a group, H a subgroup of G. Let for $g \in G$, $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$

Prove that gHg^{-1} is a subgroup of G.

Proof

Given that G is group.

H is a subgroup of G.

$gHg^{-1} = \{ghg^{-1} \mid h \in H\}$ where $g \in G$.

To prove gHg^{-1} is a subgroup of G

i.e to prove that:

(i) gHg^{-1} is nonempty subset of G.

(ii) $a, b \in gHg^{-1} \Rightarrow ab \in gHg^{-1}$

(iii) $a \in gHg^{-1} \Rightarrow a^{-1} \in gHg^{-1}$

(i) $e \in H$ [$\because H$ is a subgroup

$\Rightarrow geg^{-1} \in gHg^{-1}$

$\Rightarrow gg^{-1} \in gHg^{-1}$

$\Rightarrow e \in gHg^{-1}$

$\Rightarrow gHg^{-1}$ is nonempty

let $a \in gHg^{-1}$

$\Rightarrow a = ghg^{-1}$ where $h \in H$

Now, $g \in G, h \in H \Rightarrow g \in G, h \in G$

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

$\Rightarrow a \in G$.

So $ghg^{-1} \in G$

$\Rightarrow gHg^{-1}$ is a non-empty

(ii) $a, b \in gHg^{-1}$

$\Rightarrow a = gh_1g^{-1}, \; b = gh_2g^{-1}, \; h_1, h_2 \in H$

$\Rightarrow ab = (gh_1g^{-1})(gh_2g^{-1})$

$= g\,h_1h_2\,g^{-1}$

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

(iii) $a \in gHg^{-1}$

$\Rightarrow a = gh_1g^{-1}$, where $h_1 \in H$

$\Rightarrow a^{-1} = (gh_1g^{-1})^{-1} = \{(gh_1)g^{-1}\}^{-1}$

$= (g^{-1})^{-1}(gh_1)^{-1}$

$= g(h_1^{-1}g^{-1}) = gh_1^{-1}g^{-1}$

$\Rightarrow a^{-1} = gh_1^{-1}g^{-1} \in gHg^{-1}$

Hence gHg^{-1} is a subgroup of

2.6 Normal subgroups

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

Lemma- 2.6.1

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

Proof

($\Rightarrow$:) Given that N is a normal subgroup of G.

To prove that $gNg^{-1} = N \ \forall g \in G$.

Let $g \in G$ be arbitrary.

Claim

To prove that $gNg^{-1} = N$.

Since N is a normal subgroup of G and $g \in G$

So $gNg^{-1} \subseteq N$ —— (1), by def^n.

Now, $g \in G \Rightarrow g^{-1} \in G$

N is a normal subgroup of G and $g^{-1} \in G$

$\Rightarrow g^{-1} N (g^{-1})^{-1} \subset N$

$g^{-1} N g \subseteq N$

$\Rightarrow g g^{-1} N g g^{-1} \subseteq g N g^{-1}$

$\Rightarrow e N e \subseteq g N g^{-1}$

$\Rightarrow N \subseteq g N g^{-1}$ —— (2)

From (1) and (2) we get

$gNg^{-1} = N$

Since $g \in G$ is arbitrary.

So $gNg^{-1} = N \ \forall g \in G$.

($\Leftarrow$:)

Given that $gNg^{-1} = N \ \forall g \in G$

To prove that N is a normal subgroup of G.

We have given that

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

$\Rightarrow gNg^{-1} \subseteq N \ \forall g \in G$

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

Lemma -2.6.2

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

Proof ($\Rightarrow$:) Given that N is a subgroup of G.

Also N is a normal subgroup of G.

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

We have given that N is a normal subgroup of G

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

$\Rightarrow gNg^{-1}g = Ng \ \forall g \in G$

$\Rightarrow gNe = Ng$

$\Rightarrow gN = Ng \ \forall g \in G$

$\Rightarrow$ every left coset of N in G is a right coset of N in G.

($\Leftarrow$:) Given that N is a subgroup of G.

Also every left coset of N in G is a right coset of N in G.

To prove that N is a normal subgroup of G.

Let $gN = Nx$ —— (1)

Now $e \in N$

$\Rightarrow g \cdot e \in gN$

$\Rightarrow g \in gN$

$\Rightarrow g \in Nx$

$\Rightarrow Nx$ is a right coset of N in G containing g.

Again $e \in N$

$\Rightarrow eg \in Ng$

$\Rightarrow g \in Ng$

$\Rightarrow Ng$ is a right coset of N in G containing g.

So Nx and Ng are two right cosets of N in G containing g.

$\Rightarrow Nx \cap Ng \neq \phi$

$\Rightarrow Nx = Ng$ —— (2) $\left[\because \text{Two right cosets are either disjoint or identical} \right]$

From (1) and (2)

$gN = Ng$

$\Rightarrow gNg^{-1} = Ngg^{-1}$

$\Rightarrow gNg^{-1} = Ne$

$\Rightarrow gNg^{-1} = N$

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

Lemma - 2.6.3

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 ($\Rightarrow$):

Given that N is a subgroup of G.

Also N is a normal subgroup of G.

To prove that the product of two right cosets of N in G is a right coset of N in G.

Let Na and Nb be two right cosets of N in G.

So $a \in G$ and $b \in G \Rightarrow ab \in G$

Now, $Na\,Nb = N(aN)b$ ($\because N$ is normal, so $aN = Na$)

$= N(Na)b$

$\left[\begin{array}{l} = NNab \quad (NN = N) \\ = Nab \end{array} \right.$

which is a right coset of N in G.

$\Rightarrow Na\,Nb$ is a right coset of N in G

$\Rightarrow$ product of two right cosets of N in G is a right coset of N in G.

($\Leftarrow$): Given that N is a subgroup of G.

Also the product of two right cosets of N in G is again a right coset of N in G.

To prove that N is a normal subgroup of G.

i.e. to prove that $gng^{-1} \in N$ $\forall\, n \in N$ and $g \in G$

Let $n \in N$ and $g \in G$ be arbitrary,

Now $g \in G \Rightarrow g^{-1} \in G$,

So Ng and Ng^{-1} are two right cosets of N in G.

$\Rightarrow Ng \cdot Ng^{-1}$ is also a right coset of N in G.

clearly, $egeg^{-1} \in NgNg^{-1}$

$\Rightarrow e \in NgNg^{-1}$.

So $NgNg^{-1}$ is a right coset of N in G containing e.

Again $e \in N = Ne$.
So, N is a right coset of N in G containing e.
Hence $Ng\,Ng^{-1}$ and N are two right cosets of N in G containing e.

$\Rightarrow Ng\,Ng^{-1} \cap N \neq \phi$

$\Rightarrow Ng\,Ng^{-1} = N$ [$\because$ Two right cosets are]

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

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

$\Rightarrow gng^{-1} \in N$ [$\because n \in N \Rightarrow n^{-1} \in N$
$\Rightarrow n^{-1}N = N$]

Since $g \in G$ and $n \in N$ are arbitrary
So $gng^{-1} \in N$ $\forall g \in G$ and $n \in N$
Hence N is a normal subgroup of G.

Th-2.6.1.

If G is a group, N a normal subgroup of G, then $\frac{G}{N}$ is also a group. It is called the quotient group or factor group of G by N.

Proof

Given that G is a group and N is a normal subgroup of G.
To prove that $\frac{G}{N}$ is a group.
i.e. to prove that

1. $X, Y \in \frac{G}{N} \Rightarrow XY \in \frac{G}{N}$
2. $X, Y, Z \in \frac{G}{N} \Rightarrow (XY)Z = X(YZ)$
3. $\exists$ an element N in $\frac{G}{N}$ s.t
$XN = NX = X \quad \forall X \in \frac{G}{N}$
4. For every X in $\frac{G}{N}$ $\exists Y$ in $\frac{G}{N}$ s.t
$XY = YX = N$.

We know that $\frac{G}{N}$ is the collection of all right cosets of N in G.

1. $X, Y \in \frac{G}{N}$, where $a, b \in G$
$\Rightarrow X = Na, \; Y = Nb$.

Now $XY = NaNb$
$= N(aN)b$
$= N(Na)b$ [$\because aN = Na$ as N is normal]
$= NNab$ [$\because NN = N$]
$= Nab$

$\Rightarrow XY \in \frac{G}{N}$

2. $X, Y, Z \in \frac{G}{N}$, where $a, b, c \in G$
$\Rightarrow X = Na, \; Y = Nb, \; Z = Nc$,

$(XY)Z = \{NaNb\}Nc$
$= \{N(aN)b\}Nc$
$= \{N(Na)b\}Nc$ [$\because aN = Na$ as N is normal
$= \{NN(ab)\}Nc$
$= N(ab)Nc$
$= N\{(ab)N\}c = NN(ab)c = N(ab)c$ —— (1)

$X(YZ) = Na\{NbNc\}$
$= Na\{N(bN)c\}$
$= Na\{N(Nb)c\}$
$= Na\{NN(bc)\}$
$= Na\{Nbc\}$
$= NaNbc$
$= N(aN)bc = N(Na)bc = NN\,a(bc) = Na(bc) = N(ab)c$

From (1) and (2)

$(XY)Z = X(YZ)$

3. To prove that $\exists$ an element N in $\frac{G}{N}$ s.t

$$XN = NX = X \;\forall\; X \in \frac{G}{N}$$

First to prove that $N \in \frac{G}{N}$

let $X \in \frac{G}{N}$ be arbitrary $\Rightarrow X = Na$ where $a \in G$

Clearly, $Ne \in \frac{G}{N}$

$\Rightarrow N \in \frac{G}{N}$

Now, $XN = NaN$

$= N(aN)$

$= N(Na) = NNa = Na = X$

$NX = NNa = Na = X$

So $XN = NX = X$

(4.) To prove that for every X in $\frac{G}{N}$ $\exists$ Y in $\frac{G}{N}$

s.t $XY = YX = N$

Let $X \in \frac{G}{N}$ arbitrary

$\Rightarrow X = Na$ where $a \in G$

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

$\Rightarrow Na^{-1} \in \frac{G}{N}$

$\Rightarrow Y \in \frac{G}{N}$ $\quad$ [Let $Na^{-1} = Y$]

(1) $XY = NaNa^{-1}$

$= N(aN)a^{-1}$

$= N(Na)a^{-1}$

$= N(Na)a^{-1} = NNaa^{-1}$

$= Naa^{-1} = Ne = N$

$YX = Na^{-1}Na$

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

$= N(Na^{-1})a = NNa^{-1}a = Ne = N$

$XY = YX = N$

So for X in $\frac{G}{N}$ $\exists$ Y in $\frac{G}{N}$ s.t $XY = YX = N$

Since, $X \in \frac{G}{N}$ is arbitrary

So for every X in $\frac{G}{N}$ $\exists$ Y in $\frac{G}{N}$ s.t

$$XY = YX = N$$

$\therefore \frac{G}{N}$ is a group.

Lemma - 2.6.4

If G is a finite group and N is a normal subgroup of G then $o\left(\frac{G}{N}\right) = \frac{o(G)}{o(N)}$

Proof

Given that G is a finite group and N is a normal subgroup of G

To prove that $o\left(\frac{G}{N}\right) = \frac{o(G)}{o(N)}$

We know that $\frac{G}{N}$ is the collection of all right cosets of N in G,

$\Rightarrow o\left(\frac{G}{N}\right) =$ Number of distinct right cosets of N in G ——— (1)

Again, G is a finite group and N is a subgroup of G

$\Rightarrow \frac{o(N)}{o(G)}$, [by Lagrange's Th.]

$\Rightarrow \frac{o(G)}{o(N)} =$ Number of distinct right cosets of N in G ——— (2)

From (1) & (2)

$o\left(\frac{G}{N}\right) = \frac{o(G)}{o(N)}$

Problems

1. If H is a subgroup of G s.t the product of two right cosets of H in G is again a right coset of H in G. Prove that H is normal in G.

Proof

Given that H is a subgroup of G s.t the product of two right cosets of H in G is again a right coset of H in G.

To prove that H is normal in G.

i.e to prove that $ghg^{-1} \in H$ $\forall$ $h \in H$ & $g \in G$.

Let $h \in H$ & $g \in G$

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

So Hg and Hg^{-1} are two right cosets of H in G.

$\Rightarrow HgHg^{-1}$ is a right coset of H in G.

Now $e g e g^{-1} \in HgHg^{-1}$ ($\because e \in H$)

$\Rightarrow gg^{-1} \in HgHg^{-1}$ — (1)

$\Rightarrow e \in HgHg^{-1}$

Again $e \in H$.

Hence $HgHg^{-1}$ and H are two right cosets of H in G having a common element e.

$\Rightarrow HgHg^{-1} \cap H \neq \phi$

$\Rightarrow HgHg^{-1} = H$ [$\because$ Two right cosets are either disjoint or identical]

Now $hghg^{-1} \in HgHg^{-1}$ [$\because h \in H$]

$\Rightarrow hghg^{-1} \in H$ [$\because HgHg^{-1} = H$]

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

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

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

$\Rightarrow ghg^{-1} \in H$ [$\because h^{-1} \in H \Leftrightarrow h^{-1}H = H$]

Since $g \in G$ and $h \in H$ are arbitrary.

So $ghg^{-1} \in H$ $\forall$ $g \in G$ and $h \in H$.

Hence H is normal in G.

2. If G is a group and H is a subgroup of index 2 in G. Prove that H is a normal subgroup of G.

Proof

Given that G is a group and H is a subgroup of index 2 in G.

To prove that H is a normal subgroup of G.

i.e to prove that $Hx = xH$ $\forall$ $x \in G$.

Let $x \in G$ be arbitrary.

Now two cases arise. They are either $x \in H$ or $x \notin H$.

Case-I. If $x \in H$

$x \in H \Rightarrow Hx = H$ and $xH = H$

$Hx = xH$.

Case-II If $x \notin H$

$x \notin H \Rightarrow Hx \cap H = \phi$ ($\because$ Two right cosets are identical or disjoint.)

Since H is a subgroup of index 2 in G, so

$G = Hx \cup H = xH \cup H$

$\Rightarrow Hx \cup H = xH \cup H$

$\Rightarrow (Hx \cup H) \setminus H = (xH \cup H) \setminus H$

$Hx = xH$ $\forall x \in G$.

subgroup of G.

(3.) If N is a normal subgroup of G and H is any subgroup of G. Prove that NH is a subgroup of G.

Proof

Given that N is a normal subgroup of G.
Also, H is any subgroup of G.
To show that NH is a subgroup of G.
i.e to prove that $NH = HN$
We know that $NH = \bigcup_{h \in H} N_h$.
Since N is a normal subgroup of G.
So $N_x = xN \quad \forall x \in G$

$\Rightarrow N_h = hN \quad \forall h \in H \quad [\because H \subseteq G]$

$\Rightarrow \bigcup_{h \in H} N_h = \bigcup_{h \in H} hN$

$\Rightarrow NH = HN$

$\Rightarrow NH$ is a subgroup of G.

(4.) Show that the intersection of two normal subgroups of G is a normal subgroup of G.

Proof

Let H and K be any two normal subgroups of G.
To show that $H \cap K$ is a normal subgroup of G.
i.e to show that
(i) $H \cap K$ is a non empty subset of G.
(ii) $a, b \in H \cap K \Rightarrow ab \in H \cap K$
(iii) $a \in H \cap K \Rightarrow a^{-1} \in H \cap K$
(iv) $g \in G$, $a \in H \cap K \Rightarrow gag^{-1} \in H \cap K$

(i) Clearly $e \in H$ and $e \in K$

$\Rightarrow e \in H \cap K$

$\Rightarrow H \cap K$ is nonempty.

Let $x \in H \cap K$

$\Rightarrow x \in H$ and $x \in K \quad (\because H \subseteq G \ \& \ K \subseteq G$

$\Rightarrow x \in G$ and $x \in G$

$\Rightarrow x \in G \cap G$

$\Rightarrow x \in G$

So $H \cap K \subseteq G$.
Hence $H \cap K$ is a nonempty subset of G.

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

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

$\Rightarrow ab \in H$ and $ab \in K$

$\Rightarrow ab \in H \cap K$

(iii) $a \in H \cap K$

$\Rightarrow a \in H$ and $a \in K$

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

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

(iv) $g \in G$, $a \in H \cap K$

$\Rightarrow g \in G$, $(a \in H \ \& \ a \in K)$

$\Rightarrow (g \in G, a \in H)$ and $(g \in G, a \in K)$

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

$\left[\begin{array}{l} H \text{ is normal in } G \\ \& \ K \text{ is } \text{" in } G. \end{array} \right.$

$\Rightarrow gag^{-1} \in H \cap K$

Hence $H \cap K$ is a normal subgroup of G.

(5) If H is a subgroup of G and N is a normal subgroup of G. Show that $H \cap N$ is a normal subgroup of H.

Proof

Given that H is a subgroup of G. Also N is a normal subgroup of G. To show that $H \cap N$ is a normal subgroup of H.

Now, H and N are subgroups of G.

$\Rightarrow H \cap N$ is a subgroup of G.

$\Rightarrow$ All the four group axioms are satisfied in $H \cap N$

Again $H \cap N \subseteq H$

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

Next to show that $H \cap N$ is normal in H.

i.e to show that $hxh^{-1} \in H \cap N$ $\forall h \in H$ and $x \in H \cap N$

let $h \in H$ and $x \in H \cap N$ be arbitrary.

$\Rightarrow h \in H$ and $x \in H \cap N$

$\Rightarrow h \in H$ and $(x \in H$ and $x \in N)$

$\Rightarrow (h \in H$ and $x \in H)$ and $(h \in H$ and $x \in N)$

$\Rightarrow (h \in H, x \in H, h^{-1} \in H)$ and $(h \in G$ and $x \in N)$

$\{\because H \subseteq G$ and H is a subgroup of $G\}$

$\Rightarrow hxh^{-1} \in H$ and $hxh^{-1} \in N$

$\Rightarrow hxh^{-1} \in H \cap N$

So $hxh^{-1} \in H \cap N$ $\forall h \in H$ and $\in H \cap N$.

Hence $H \cap N$ is normal in H.

Therefore $H \cap N$ is a normal subgroup of H.

(6) Show that every subgroup of an abelian group is normal.

Proof

To show that every subgroup of an abelian group is normal in group.

let H be any subgroup of an abelian group G.

Claim :- To show that H is normal in G.

i.e to show that $ghg^{-1} \in H$ $\forall g \in G$ & $h \in H$

Let $g \in G$ & $h \in H$ be arbitrary.

Now $ghg^{-1} = hgg^{-1}$ ($\because G$ is abelian so $gh = hg$)

$= he$ (existence of inverse)

$= h$ (" identity)

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

Since $g \in G$ and $h \in H$ are arbitrary.

So $ghg^{-1} \in H$ $\forall g \in G$ and $h \in H$.

Hence H is normal in G.

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

Proof

Given that N and M are normal subgroup of G.

To prove that NM is a normal subgroup of G.

We know that $NM = \bigcup_{m \in M} Nm$.

Since N is normal in G, so,

$Ng = gN$ $\forall g \in G$

$\Rightarrow Nm = mN$ $\forall m \in M$ ($\because M \subseteq G$)

$\Rightarrow \bigcup_{m \in M} N_m = \bigcup_{m \in M} mN$

$\Rightarrow NM = MN$

$\Rightarrow NM$ is a subgroup of G.

Next to show that NM is normal in G

i.e to show that $x(nm)x^{-1} \in NM \ \forall x \in G$ and $nm \in NM$.

$x(nm)x^{-1}$

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

$= x(nx^{-1}xm)x^{-1}$

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

[$\because$ N is normal in G and $x \in G$, $n \in N$. So, $xnx^{-1} \in N$

Again M is normal in G and $x \in G$, $m \in M$

So, $xmx^{-1} \in M$]

So, $x(nm)x^{-1} \in NM \ \forall x \in G$ and $nm \in NM$

So NM is normal in G.

2.7 Homomorphisms

Def^n:- A mapping ϕ from a group G into a group $\bar{G}$ is said to be a homomorphism if $\phi(ab) = \phi(a)\phi(b) \ \forall a, b \in G$.

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

Given that G is a group and N is a normal subgroup of G. ϕ from G to $\frac{G}{N}$ is defined by

A mapping ϕ from G to $\frac{G}{N}$

$\phi(x) = Nx \quad \forall x \in G$

To prove that ϕ is a homomorphism of G onto $\frac{G}{N}$

First to prove that $\phi: G \to \frac{G}{N}$ is a homomorphism

To prove that $\phi(xy) = \phi(x)\phi(y) \ \forall x, y \in G$.

Let $x, y \in G$.

so $xy \in G$

By def^n $\phi(x) = Nx$ & $\phi(y) = Ny$

$\phi(xy) = Nxy$

Now $\phi(xy) = Nxy$

$= N\,Nxy$

$= N(Nx)y$

$= N(xN)y \quad [\because N$ is normal$]$

$= NxNy$

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

$\Rightarrow \phi(xy) = \phi(x)\,\phi(y)$

Since $x, y \in G$ are arbitrary

So, $\phi(xy) = \phi(x)\cdot\phi(y) \ \forall x, y \in G$

Hence $\phi : G \to \frac{G}{N}$ is homomorphism.

Next to prove that $\phi : G \to \frac{G}{N}$ is onto.

i.e. to prove that for every Y in $\frac{G}{N}$ $\exists$ an element x in G s.t. $Y = \phi(x)$

let $Y \in \frac{G}{N}$ be arbitrary.

$\Rightarrow Y = Nx$ where $x \in G$

By defn of ϕ, $\phi(x) = Nx = Y$

So for Y in $\frac{G}{N}$ $\exists\, x$ in G s.t. $Y = \phi(x)$.

Since $Y \in \frac{G}{N}$ is arbitrary

So for every Y in $\frac{G}{N}$ $\exists\, x$ in G s.t.

$Y = \phi(x)$

Hence $\phi : G \to \frac{G}{N}$ is onto.

$\therefore \phi : G \to \frac{G}{N}$ is a homomorphism and onto.

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 $\forall x \in G$.

Proof

1. Given that ϕ is a homomorphism of G into $\bar{G}$

To prove that $\phi(e) = \bar{e}$

$x \cdot e = x$

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

$\Rightarrow \phi(x)\cdot\phi(e) = \phi(x)$ — ① (ϕ is a homomorphism)

Again $\phi(x)\cdot\bar{e} = \phi(x)$ — ②, (Existence of identity element in $\bar{G}$)

From ① and ② we get

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

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

2. Given that ϕ is a homomorphism of G into $\bar{G}$

To prove that

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

$x \cdot x^{-1} = e$ [existence of inverse element in G]

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

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

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

Again $\phi(x)\cdot\phi(x)^{-1} = \bar{e}$ — ② [Existence of inverse element in $\bar{G}$]

From ① and ②

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

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

Defn. (Kernel of a homomorphism).

let ϕ be a homomorphism of G into $\bar{G}$. The kernel of ϕ is denoted by K_ϕ and is defined by

$$K_\phi = \{x \in G \,/\, \phi(x) = \bar{e}\}.$$

Lemma - 2.7.3

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

Proof

Given that ϕ is a homomorphism of G onto $\bar{G}$ with Kernel K.

To prove that K is a normal subgroup of G.

i.e to prove that

(1) K is a nonempty subset of G.

(2) $x, y \in K \Rightarrow xy \in K$

(3) $x \in K \Rightarrow x^{-1} \in K$

(4) $gkg^{-1} \in K \;\forall\; k \in K$ and $g \in G$.

(1) To prove that K is a nonempty subset of G.

We know that

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

$\Rightarrow e \in K$

$\Rightarrow K$ is nonempty.

From defn of Kernel

$K = \{x \in G \mid \phi(x) = \bar{e}\}$

$\Rightarrow K \subseteq G$

Hence K is a nonempty subset of G.

(2) To prove that $x, y \in K \Rightarrow xy \in K$

$x, y \in K$

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

$\Rightarrow \phi(x) \cdot \phi(y) = \bar{e}\,\bar{e}$ [$\because \phi$ is a homomorphism]

$\Rightarrow xy \in K$

(3) To prove that $x \in K \Rightarrow x^{-1} \in K$

$x \in K$

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

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

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

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

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

(4) To prove that $gkg^{-1} \in K \;\forall\; k \in K$ and $g \in G$. Let $k \in K$ and $g \in G$ be arbitrary $g \in G$,

Now $\phi(gkg^{-1})$

$= \phi(g)\,\phi(k)\,\phi(g^{-1})$ [$\because \phi$ is a homomorphism]

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

$= \phi(g) \cdot \phi(g^{-1})$ [$\because \phi$ is a homomorphism]

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

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

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

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

Since $k \in K$ and $g \in G$ are arbitrary

So $gkg^{-1} \in K \;\forall\; k \in K, g \in G$

$\therefore K$ is a normal subgroup of G.

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 in G is given by Kx, where x is any particular inverse image of $\bar{g}$ in G.

Proof

Given that $\phi : G \to \bar{G}$ is a homomorphism and onto K is the Kernel of ϕ.

x is any particular inverse image of $\bar{g}$ under ϕ.

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

i.e. $\phi(x) = \bar{g}$

To prove that Kx is the set of all inverse images of $\bar{g}$ under ϕ. i.e. to prove that

(1) Any element in Kx is an inverse image of $\bar{g}$ under ϕ.

(2) Any inverse image of $\bar{g}$ under ϕ is an element of Kx.

To prove that

(1) Any element in Kx is an inverse image of $\bar{g}$ under ϕ.

let y be any element in Kx

$\Rightarrow y \in Kx$

$\Rightarrow y = kx$ (where $k \in K$)

Now $\phi(y) = \phi(kx)$ $(\because y = kx)$ $(\because \phi$ is a homomorphism$)$

$= \phi(k) \cdot \phi(x)$ $(\because k \in K)$

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

$= \phi(x)$

$= \bar{g}$ $(\because \phi(x) = \bar{g})$

$\Rightarrow \phi(y) = \bar{g}$

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

$\Rightarrow y$ is an inverse image of $\bar{g}$ under ϕ

Since y is any element in Kx. So every element in Kx is an inverse image of $\bar{g}$ under ϕ.

(2) To prove that

Any inverse image of $\bar{g}$ under ϕ is an element of Kx.

let z, be any inverse image of $\bar{g}$ under ϕ

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

$\Rightarrow \phi(z) = \bar{g}$

$\Rightarrow \phi(z) = \phi(x)$ $(\because \phi(x) = \bar{g})$

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

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

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

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

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

$\Rightarrow z \cdot x^{-1} \cdot x \in Kx$

$\Rightarrow z \in Kx$

Since z is any inverse image of $\bar{g}$ under ϕ. So, any inverse element of $\bar{g}$ under ϕ is an element of Kx.

K_n is the set of all inverse image of $\bar{g}$ under ϕ.

Defn:- A homomorphism ϕ from G onto $\bar{G}$ is said to be an isomorphism if ϕ is one-to-one.

Corollary

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

Proof ($\Rightarrow$)

Given that ϕ is a homomorphism of G into $\bar{G}$ with kernel $K\phi$.

Also ϕ is an isomorphism of G onto $\bar{G}$

To prove that $K_\phi = (e)$

Assume that $K_\phi \neq (e)$

$\Rightarrow \exists$ at least one element a in K_ϕ s.t $a \neq e$

$\Rightarrow a \in K_\phi$

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

$\Rightarrow \phi(a) = \phi(e)$ $\quad (\because \phi(e) = \bar{e})$

$\Rightarrow a = e$ $\quad (\because \phi$ is one-one$)$

Hence our assumption is wrong.

So $K_\phi = (e)$

($\Leftarrow$) Given that ϕ is a homomorphism of G into $\bar{G}$ with kernel K_ϕ.

Also $K_\phi = (e)$

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

Since $\phi : G \to \bar{G}$ is given to be a homomorphism.

So we have only to prove that $\phi : G \to \bar{G}$ is one-one

i.e to prove that $\phi(a) = \phi(b) \Rightarrow a = b$

$\Rightarrow \phi(a) = \phi(b)$

$\Rightarrow \phi(a)\,\phi(b)^{-1} = \phi(b)\,\phi(b)^{-1}$ (Existence of inverse element in $\bar{G}$)

$\Rightarrow \phi(a)\,\phi(b^{-1}) = \bar{e}$, ϕ is a homomorphism

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

$\Rightarrow ab^{-1} \in K_\phi$

$\Rightarrow ab^{-1} = e$ $\quad (\because K_\phi = (e))$

$\Rightarrow a = b$

So, $\phi(a) = \phi(b) \Rightarrow a = b$

Hence $\phi : G \to \bar{G}$ is one one.

Hence $\phi : G \to \bar{G}$ is isomorphism.

Th- 2.7.1

Let ϕ be a homomorphism of G onto $\bar{G}$ with kernel K. Then $\frac{G}{K} \approx \bar{G}$.

Proof

Given that ϕ is a homomorphism of G onto $\bar{G}$ with kernel K.

To prove that $\frac{G}{K} \approx \bar{G}$

Let the homomorphism $\phi : G \to \bar{G}$ be defined by

$$\phi(g) = \bar{g} \quad \forall \; g \in G \quad \text{--- (1)}$$

Let $\psi : \frac{G}{K} \to \bar{G}$ be defined by

$$\psi(Kg) = \bar{g} \quad \forall\ Kg \in \frac{G}{K} \quad \text{---} (2)$$

From (1) and (2) we get

$$\psi(Kg) = \phi(g) \quad \text{---} (3)$$

Claim: To prove that

1. $\psi: \frac{G}{K} \to \bar{G}$ is well defined
2. $\psi: \frac{G}{K} \to \bar{G}$ is a homomorphism
3. $\psi: \frac{G}{K} \to \bar{G}$ is one-one
4. $\psi: \frac{G}{K} \to \bar{G}$ is onto

1. To prove that $\psi: \frac{G}{K} \to \bar{G}$ is well defined

i.e. to prove that

$$Kg_1 = Kg_2 \Rightarrow \psi(Kg_1) = \psi(Kg_2)$$

$Kg_1 = Kg_2$ where $g_2 = kg_2,\ k \in K$

Now, $kg_1 = g_2$

$\Rightarrow \phi(kg_1) = \phi(g_2)$

$\Rightarrow \phi(k) \cdot \phi(g_1) = \phi(g_2)$ $\quad$ $\because \phi$ is homomorphism

$\Rightarrow \bar{e}\ \phi(g_1) = \phi(g_2)$ $\quad$ ($\because k \in K$, so $\phi(k) = \bar{e}$)

$\Rightarrow \phi(g_1) = \phi(g_2)$, $\quad$ Existence of identity element in $\bar{G}$.

$\Rightarrow \psi(Kg_1) = \psi(Kg_2)$

So, $Kg_1 = Kg_2 \Rightarrow \psi(Kg_1) = \psi(Kg_2)$.

Hence $\psi: \frac{G}{K} \to \bar{G}$ is well defined.

(2) To prove that $\psi: \frac{G}{K} \to \bar{G}$ is a homomorphism

i.e. to prove that

$$\psi(Kg_1 Kg_2) = \psi(Kg_1)\psi(Kg_2)$$

L.H.S $\psi(Kg_1 Kg_2)$

$= \psi(Kg_1g_2)$ ($\because K$ is normal so $g_1K = Kg_1$)

$= \psi(Kg_1g_2)$ ($\because KK = K$)

$= \phi(g_1g_2)$

$= \phi(g_1)\phi(g_2)$

$= \psi(Kg_1)\psi(Kg_2)$

So $\psi: \frac{G}{K} \to \bar{G}$ is a homomorphism.

(3) To prove that $\psi: \frac{G}{K} \in \bar{G}$ is one-one

i.e. to prove that

$$\psi(Kg_1) = \psi(Kg_2) \Rightarrow Kg_1 = Kg_2$$

$\psi(Kg_1) = \psi(Kg_2)$

$\Rightarrow \phi(g_1) = \phi(g_2)$, by eqn-3

$\Rightarrow \phi(g_1)\phi(g_2)^{-1} = \phi(g_2)\phi(g_2)^{-1}$

$\Rightarrow \phi(g_1) \cdot \phi(g_2)^{-1} = \bar{e}$

$\Rightarrow \phi(g_1)\ \phi(g_2^{-1}) = \bar{e}$ $\quad$ [$\because \phi(a^{-1}) = \phi(a)^{-1}$]

$\Rightarrow \phi(g_1 g_2^{-1}) = \bar{e}$ $\quad$ [ϕ is homomorphism]

$\Rightarrow g_1 g_2^{-1} \in K$ $\quad$ by defn of kernel

$\Rightarrow Kg_1g_2^{-1} = K$ $\quad$ [$\because a \in H \Leftrightarrow Ha = H$]

$\Rightarrow Kg_1 = Kg_2$

Hence $\psi: \frac{G}{K} \to \bar{G}$ is one-one.

(4) To prove that $\psi: \bar{G}$ is onto i.e. to prove that

For every $\bar{g}$ in $\bar{G}$ $\exists$ an element Kg in $\frac{G}{K}$

s.t $\bar{g} = \psi(Kg)$

Let $\bar{g} \in \bar{G}$ be arbitrary.

Since $\phi: G \to \bar{G}$ is onto and $\bar{g} \in \bar{G}$

So, $\exists$ an element g in G s.t

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

Now, $g \in G \Rightarrow Kg \in \frac{G}{K}$

We have $\bar{g} = \phi(g)$

$$= \psi(Kg)$$

$$\Rightarrow \bar{g} = \psi(Kg)$$

So $\psi: \frac{G}{K} \to \bar{G}$ is onto

Hence $\psi: \frac{G}{K} \to \bar{G}$ a homomorphism, one-one and onto.

$$\text{So } \frac{G}{K} \approx \bar{G}$$

Th- 2.7.2

Let ϕ be a homomorphism of G onto $\bar{G}$ with Kernel K and let $\bar{N}$ be a normal subgroup of $\bar{G}$.

$N = \{x \in G \mid \phi(x) \in \bar{N}\}$. Then $\frac{G}{N} \approx \frac{\bar{G}}{\bar{N}}$

Equivalently, $\frac{G}{N} \approx \frac{G/K}{N/K}$

Proof

Given that ϕ is a homomorphism of G onto $\bar{G}$ with Kernel K.

$\bar{N}$ is a normal subgroup of $\bar{G}$.

$$N = \{x \in G \mid \phi(x) \in \bar{N}\}$$

To prove that $\frac{G}{N} \approx \frac{\bar{G}}{\bar{N}}$

Let the homomorphism $\phi: G \to \bar{G}$ is defined by

$$\phi(g) = \bar{g} \quad \forall g \in G \quad \text{—— (1)}$$

Let $\psi: G \to \frac{\bar{G}}{\bar{N}}$ be defined by

$$\psi(g) = \bar{N}\bar{g} \quad \forall g \in G \quad \text{—— (2)}$$

From (1) and (2) we get

$$\psi(g) = \bar{N}\phi(g) \quad \text{—— (3)}$$

Claim To prove that

1. $\psi: G \to \frac{\bar{G}}{\bar{N}}$ is well defined
2. $\psi: G \to \frac{\bar{G}}{\bar{N}}$ is a homomorphism
3. $\psi: G \to \frac{\bar{G}}{\bar{N}}$ is onto

1. To prove that $\psi: G \to \frac{\bar{G}}{\bar{N}}$ is well defined

i.e to prove that

$a = b \Rightarrow \psi(a) = \psi(b)$

$a = b$ (∵ ϕ is a mapping)

$\Rightarrow \phi(a) = \phi(b)$

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

$\Rightarrow \psi(a) = \psi(b)$

Hence $\psi: G \to \frac{\bar{G}}{\bar{N}}$ is well defined.

(2) To prove that $\psi: G \to \frac{\bar{G}}{\bar{N}}$ is a homomorphism

i.e to prove that

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

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

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

$$= \bar{N}\bar{N}\phi(a)\phi(b) \quad (\because \bar{N}\bar{N} = \bar{N})$$

$$= \bar{N}\phi(a)\bar{N}(b) \quad (\because \bar{N} \text{ is normal})$$

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

So $\psi: G \to \frac{\bar{G}}{\bar{N}}$ is a homomorphism.

(5) To prove that $\psi : G \to \frac{\bar{G}}{\bar{N}}$ is onto

to prove that for every $\bar{N}\bar{g}$ in $\frac{\bar{G}}{\bar{N}}$ $\exists$ an element g in G s.t

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

Let $\bar{N}\bar{g} \in \frac{\bar{G}}{\bar{N}}$ be arbitrary

$\bar{N}\bar{g} \in \frac{\bar{G}}{\bar{N}}$

$\Rightarrow \bar{g} \in \bar{G}$

Since $\phi : G \to \bar{G}$ is onto and $\bar{g} \in \bar{G}$

So, $\exists$ an element g in G s.t $\bar{g} = \phi(g)$

By def^n of ψ

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

for $\bar{N}\bar{g}$ in $\frac{\bar{G}}{\bar{N}}$, $\exists$ an element g in G s.t $\bar{N}\bar{g} = \psi(g)$

Since $\bar{N}\bar{g} \in \frac{\bar{G}}{\bar{N}}$ is arbitrary, so for every $\bar{N}\bar{g}$ in $\frac{\bar{G}}{\bar{N}}$ $\exists$ an element g in G s.t $\bar{N}\bar{g} = \psi(g)$

$\Rightarrow \psi : G \to \frac{\bar{G}}{\bar{N}}$ is onto

So, ψ is a homomorphism of G onto $\frac{\bar{G}}{\bar{N}}$

$\Rightarrow \frac{G}{K_\psi} \approx \frac{\bar{G}}{\bar{N}}$

Claim: To prove that $K_\psi = N$

Let $x \in K_\psi$

$\Leftrightarrow \psi(x) = \bar{N}$

$\Leftrightarrow \bar{N}\phi(x) = \bar{N}$

$\Leftrightarrow \phi(x) \in \bar{N}$ $\quad (\because a \in H \Leftrightarrow Ha = H)$

$\Leftrightarrow x \in N$

Consequently

$K_\psi \subseteq N$ and $N \subseteq K_\psi$

Hence $K_\psi = N$

$\therefore \frac{G}{N} \approx \frac{\bar{G}}{\bar{N}}$

Next, to prove that $\frac{G}{N} \approx \frac{\left(\frac{G}{K}\right)}{\left(\frac{N}{K}\right)}$

We have given that ϕ is a homomorphism of G onto $\bar{G}$ with Kernel K,

$\Rightarrow \frac{G}{K} \approx \bar{G}$

Also, ϕ is a homomorphism of N onto $\bar{N}$ with Kernel K,

$\Rightarrow \frac{N}{K} \approx \bar{N}$

Hence $\frac{\frac{G}{K}}{\frac{N}{K}} \approx \frac{\bar{G}}{\bar{N}}$

$\Rightarrow \frac{\bar{G}}{\bar{N}} \approx \frac{G/K}{N/K}$, By Symmetry

Now $\frac{G}{N} \approx \frac{\bar{G}}{\bar{N}}$ and $\frac{\bar{G}}{\bar{N}} \approx \frac{G/K}{N/K}$

Hence $\frac{G}{N} \approx \frac{(G/K)}{(N/K)}$

2.7

Q1(e) G is any abelian group $\phi: G \to G$ is defined by $\phi(x) = x^5 \; \forall \; x \in G$

$\phi(xy) = (xy)^5$

$= x^5 y^5 = \phi(x)\,\phi(y)$

$\therefore \phi$ is a homomorphism,

Now, $\phi(x) = \phi(y)$

$\Rightarrow x^5 = y^5$

$\Rightarrow x = y$

$\therefore \phi$ is one-one

$\phi = K_\phi = \{e\}$

(2) Given G is any group

g is a fixed element in G,

$\phi: G \to G$ is defined by $\phi(x) = gxg^{-1}$

To prove ϕ is an isomorphism of G onto G,

i.e. to prove that

(i) ϕ is well-defined.

(ii) ϕ is a homomorphism,

(iii) ϕ is one-one

(iv) ϕ is onto.

(i) If $x = y$

$\Rightarrow gx = gy$

$\Rightarrow gxg^{-1} = gyg^{-1}$

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

Hence ϕ is well defined.

(ii) To show that ϕ is homomorphism

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

$= gx(g^{-1}g)yg^{-1}$

$= (gxg^{-1})(gyg^{-1}) = \phi(x)\,\phi(y)$

(iii) If $\phi(x) = \phi(y)$

$\Rightarrow gxg^{-1} = gyg^{-1}$

$\Rightarrow x = y.$

So $\phi: G \to G$ is one-one.

So $\phi: G \to G$ is onto

(iv) To show $\phi: G \to G$ is onto

i.e to show that for every y in G $\exists$ x in G s.t $y = \phi(x)$

Let $y \in G$ be arbitrary.

$\Rightarrow g^{-1}yg \in G.$

Let $g^{-1}yg = x$

So $x \in G$

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

$= gg^{-1}\,y\,gg^{-1}$

$= eye = y$

So for $y \in G$ $\exists$ $x \in G$ s.t $y = \phi(x)$.

$\therefore \phi$ is onto.

Hence ϕ is an isomorphism of G onto G.