Set-VI

Homomorphisms, Isomorphisms of Groups:

→ Let $(G, \cdot)$, $(G', *)$ be two groups.
A mapping $f: G \to G'$ is called a homomorphism, if
$f(a \cdot b) = f(a) * f(b)$. $\forall a, b \in G$.

In other words, a homomorphism preserves the compositions in the groups G and G'.
However, if we are not specific about the compositions of the groups G and G', we say that a mapping $f: G \to G'$ is a homomorphism, if
$f(ab) = f(a) \cdot f(b)$ ——— (1)
$\forall a, b \in G$

Note: In equation (1), the product ab on LHS takes place in G, while the product $f(a) \cdot f(b)$ on RHS takes place in G'.

→ If $f: G \to G'$ is a homomorphism and onto then the group G' is said to be a homomorphic image of a group G or f is said to be a homomorphism G onto G'. we write this as $f(G) = G'$. In this case write $G \simeq G'$.
(read as G is homomorphic to G')
— Homomorphism onto sometimes called as ephimorphism.

→ Let G, G' be two groups. If $f: G \to G'$ is homomorphism and one-one then f is called isomorphism from $G \to G'$.

→ If $f: G \to G'$ is homomorphism, one-one and onto then G' is called isomorphic image of G (or G is isomorphic to G' and we write $G \cong G'$.

Note: If the group G is finite then G can be isomorphic to G', only if G' is also finite and the number of elements in G is equal to the number of elements in G'.

otherwise there will exist no mapping from G to G' which is one-one and onto.

→ A homomorphism of a group G into itself is called an endomorphism.

→ An isomorphism of a group into itself is called an automorphism.

1-1 homomorphism = Isomorphism

1-1 endomorphism = Automorphism.

Examples:

Let $G=(\mathbb{Z},+)$ and $G'=\{2^n / n\in\mathbb{Z}\}$, where G' is a group w.r.t x^n.

Now we define a mapping, $f: G \to G'$ such that

$$f(n) = 2^n \quad \forall n \in \mathbb{Z}.$$

Now for all $n_1, n_2 \in G$

$$\Rightarrow n_1+n_2 \in G \text{ and } f(n_1)=2^{n_1},\ f(n_2)=2^{n_2}$$

Now we have

$$f(n_1+n_2) = 2^{n_1+n_2} \quad (\text{by defn})$$
$$= 2^{n_1}.2^{n_2}$$
$$= f(n_1).f(n_2)$$

$$\therefore f(n_1+n_2) = f(n_1).f(n_2) \quad \forall n_1, n_2 \in G.$$

$\therefore f$ is homomorphism.

To show f is 1-1:

Let $n_1, n_2 \in G$. then we have $f(n_1)=f(n_2)$.

$$\Rightarrow 2^{n_1}=2^{n_2}$$
$$\Rightarrow n_1=n_2$$
$$\therefore f \text{ is } 1\text{-}1.$$

$\therefore f$ is an isomorphism.

→ $G=\mathbb{R}^+$ is a group under x^n and $G'=\mathbb{R}$ is a group under $+^n$.

Sol^n: Now we define a mapping, $f: G \to G'$

Such that $f(x) = \log_{10} x$ ~~$\forall x \in G$~~.

Now for all $x_1, x_2 \in G \Rightarrow x_1 \cdot x_2 \in G$ and $f(x_1) = \log_{10} x_1$

$f(x_2) = \log_{10} x_2$

Now we have

$$f(x_1 \cdot x_2) = \log_{10}(x_1 \cdot x_2) \quad \text{(by defn)}$$
$$= \log_{10} x_1 + \log_{10} x_2$$
$$= f(x_1) + f(x_2)$$

$\therefore f$ is homomorphism.

TO show f is 1-1:

we have $f(x_1) = f(x_2)$. ~~$\forall x_1, x_2 \in G$~~.

$\Rightarrow \log_{10} x_1 = \log_{10} x_2$

$\Rightarrow x_1 = x_2$

$\therefore f$ is 1-1

$\therefore f$ is isomorphism.

TO show f is onto:

Let $y \in G' = \mathbb{R}$.

$\therefore 10^y$ is a +ve real number.

$\Rightarrow 10^y \in G = \mathbb{R}^+$.

$$\therefore f(10^y) = \log_{10} 10^y$$
$$= y \log_{10} 10$$
$$= y(1)$$
$$= y.$$

$\therefore f(10^y) = y$.

$\therefore$ for every $y \in G'$, $\exists\ 10^y \in G$ such that $f(10^y) = y$.

$\therefore f$ is onto.

G' is isomorphic image of G.

Properties of homomorphisms

Theorem Let $(G, \cdot)$, $(G', \cdot)$ be two groups. Let f be a homomorphism from G into G' then

(i) $f(e) = e'$ where 'e' is the identity in G and e' is the identity in G'.

(ii) $f(\bar{a}^1) = [f(a)]^{-1}$ $\forall a \in G$.

proof: (i) $f(e) = f(ee)$

$\Rightarrow f(ee) = f(e)$

$\Rightarrow f(e).f(e) = e' f(e)$ ($\because$ f is homomorphism and $e', f(e) \in G'$)

$\Rightarrow f(e) = e'$ (By RCL in G').

(ii) Let $a \in G \Rightarrow \bar{a}^1 \in G$ and $a\bar{a}^1 = e$.

Now we have

$f(a\bar{a}^1) = f(a).f(\bar{a}^1)$

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

$= f(e)$

$= e'$ where $f(a), f(a^{-1}), f(e) \in G'$

$\therefore f(a) f(\bar{a}^1) = e'$

$$f(\bar{a}^1) = [f(a)]^{-1}$$

Theorem (2) If f is a homomorphism from a group $(G, \cdot)$ into $(G', \cdot)$ then $(f(G), \cdot)$ is a subgroup of G'.

proof: By defn $f(G) = \{f(a) / a \in G\}$ and $f(G) \subseteq G'$

Let $a', b' \in f(G)$

$\therefore \exists\ a, b \in G$ such that $f(a) = a'$ & $f(b) = b'$.

Now $a'.(b')^{-1} = f(a).[f(b)]^{-1} = f(a).f(b^{-1})$

$= f(ab^{-1})$ ($\because$ f is homo.)

$\in f(G)$ ($\because a, b \in G \Rightarrow ab^{-1} \in G$)

$\therefore a'(b')^{-1} \in f(G)$ $\forall a', b' \in f(G)$

$\therefore f(G)$ is a subgroup of G'.

i.e. the homomorphic image of the group G

is a subgroup of G'.
i.e, the homomorphic image of a group is a group.

Theorem ② Every homomorphic image of an abelian group G is abelian.

proof: Let $(G,\cdot)$ be an abelian group. and $(G',\cdot)$ be a group.
Let $f: G \to G'$ be a homomorphism and onto.
$\therefore G'$ is the homomorphic image of G.
i.e $G' = f(G)$.

Let $a', b' \in G'$
$\therefore \exists$ elements $a, b \in G$ such that $f(a) = a'$ & $f(b) = b'$.

Since G is abelian.
$\therefore ab = ba$.

Now $a'b' = f(a)f(b)$
$= f(ab)$
$= f(ba)$
$= f(b) \cdot f(a)$
$= b' \cdot a'$.

$\therefore a'b' = ba'. \quad \forall a', b' \in G'$
$\therefore G'$ is an abelian.

Note: The converse of the above theorem need not be true.
i.e, If the homomorphic image of a group G is abelian. then the group need not be abelian.

Ex: P_3 is non-abelian group.
A_3 is normal subgroup of P_3.
The quotient group $\frac{P_3}{A_3}$ is a homomorphic image of P_3.
Now $\frac{P_3}{A_3}$ is of order 2 and is abelian.

Note: Even f is an isomorphism:
(i) Substitute 'isomorphism' for homomorphism in Theorem ① and it is true. The same proof holds

(ii) Substitute 'isomorphism' for homomorphism in Theorem ② and it is true. The same proof holds.

(iii) Substitute isomorphism onto for homomorphism onto in Theorem ③ and it is true. The same proof holds.

The converse of the theorem is [redacted] true.

Theorem Let G be a group and G' be a non-empty set. If there exists a mapping f from G onto G' such that $f(ab) = f(a) \cdot f(b)$ for $a, b \in G$ then G' is a group.

proof: $f: G \to G'$ is onto such that $f(ab) = f(a) \cdot f(b)$ $\forall a, b \in G$.

TO prove that G' is a group.

(i) Closure prop:

Let $a', b' \in G'$.

Since f is onto, $\exists\ a, b \in G$ such that

$$f(a) = a' \ \& \ f(b) = b'.$$

Also $ab \in G \Rightarrow f(ab) \in G'$.

$$\therefore a'b' = f(a)\,f(b) = f(ab) \in G'$$

$$\therefore a'b' \in G'.$$

(ii) Asso. prop:

Let $a', b', c' \in G'$.

Since f is onto, $\exists\ a, b, c \in G$ such that

$f(a) = a'$, $f(b) = b'$, $f(c) = c'$.

$$\text{Now } a'(b'c') = (f(a) \cdot f(b)) \cdot f(c)$$

$$= f(ab) \cdot f(c) \quad \text{by defn}$$

$$= f[(ab)c]$$

$$= f[a(bc)] \quad (\because G \text{ is group})$$

$$= f(a) \cdot f(bc)$$

$$= f(a)\,[f(b) \cdot f(c)]$$

$$= a'(b'c')$$

$\therefore G'$ is Asso.

Existence of left identity:

Let $a' \in G'$.
Let e be the identity element in G.
Since f is onto,
$\therefore f(e) = e' \in G'$, $\exists\, a \in G$ such that $f(a) = a'$.

Now $e'a' = f(e)\, f(a)$
$= f(ea)$
$= f(a)$ $(\because ea = a \ \forall a \in G)$
$= a'$.
$\therefore e'a' = a'$
$\therefore$ Identity exists in G' and it is $f(e) = e'$.

Existence of left inverse:

Let $a' \in G'$, $\exists\, a \in G$ such that $f(a) = a'$.
$\therefore \bar{a}^1 \in G$ and $f(\bar{a}^1) \in G'$.
Now $f(\bar{a}^1)\, a' = f(\bar{a}^1)\, f(a)$
$= f(\bar{a}^1 a)$
$= f(e)$
$= e'$.
$\therefore f(\bar{a}^1)\, a' = e'$
$\therefore f(\bar{a}^1)$ is the inverse of a' in G'.
$\therefore$ Every element of G' is invertible.
$\therefore$ G' is a group.

Note: when f is a one-one mapping from G into G', this theorem is not true.

Kernel of a Homomorphism:

Let G & G' be two groups, $f: G \to G'$ be a homomorphism then the set 'K' of all those elements of G whose image is the identity element e' of G' is called the kernel of the homomorphism 'f'.

i.e., Kernel $f = \{ x \in G \mid f(x) = e' \} = K$.

— Sometimes Kernel f is written as $\ker f$.

Note: If $e \in G$ then $f(e) = e'$.
i.e, $e \in \ker f$.
$\therefore$ $\ker f$ is non-empty.

Ex①: The function $f: (\mathbb{R}^+, \cdot) \to (\mathbb{R}, +)$ such that $f(x) = \log_a x$ $\forall x \in \mathbb{R}^+$ is a homomorphism.
'0' is the identity element in $\mathbb{R}$,
$f(1) = \log_a 1 = 0$ (identity in $\mathbb{R}$)
$\therefore$ 1 is the only element with this property.
$\therefore \ker f = \{1\}$.

Ex②: The function $f: (\mathbb{R}, +) \to (\mathbb{R}^+, \times)$ defined as $f(x) = a^x$; $a > 0$ and $a \neq 1$. and its homomorphism.
$f(0) = a^0 = 1$ (identity in $\mathbb{R}^+$)
$\therefore$ 0 is the only element with this property.
$\therefore$ $\ker f = \{0\}$.

Ex③ Let $G = I$ is a group w.r.t $+^n$.
$G' = \{1, -1\}$ is a group w.r.t $\times^n$.
Define $f: G \to G'$ as follows:
$f(n) = 1$, n is even
$= -1$, n is odd.
1 is the identity element in G'.
TO prove f is homomorphism:
Let $n_1, n_2 \in G$ then we have the following possibilities:
Case(i): Both n_1 and n_2 are even.
$\therefore n_1 + n_2$ is even.
$\therefore f(n_1) = 1$, $f(n_2) = 1$
$\therefore f(n_1 + n_2) = 1$ ($\because n_1 + n_2$ is even)
$= 1 \cdot 1$.
$= f(n_1) \cdot f(n_2)$

Case(ii): One of n_1, n_2 is even and other is odd.

Let n_1 be even and n_2 be odd.

$\therefore n_1+n_2$ is odd.

$\therefore f(n_1)=1$, $f(n_2)=-1$

Now $f(n_1+n_2)=-1$.

$= 1.(-1)$

$= f(n_1).f(n_2)$.

Case(iii): Both n_1 & n_2 are odd.

$\therefore n_1+n_2$ is even.

$f(n_1)=-1$, $f(n_2)=-1$

Now $f(n_1+n_2)=+1$

$=(-1)(-1)$

$= f(n_1)f(n_2)$

$\therefore$ f is a homomorphism from $G \to G'$.

$\therefore \ker f = \{n \mid n \text{ is even}\}$.

2008

Theorem: If f is a homomorphism of a group G into a group G' then the kernel of f is a normal subgroup of G.

proof: Let e be the identity element in G and e' be the identity element in G'. and $f: G \to G'$ is a homomorphism.

Let $K = \ker f$ then $K = \{x \in G / f(x) = e'\}$.

Since $e \in G$

$f(e) = e' \Rightarrow e \in K$.

$\therefore K$ is non-empty subset of G.

Let $a, b \in K$ then $f(a)=e'$, $f(b)=e'$.

Now $f(ab^{-1}) = f(a).f(b^{-1})$

$= f(a)[f(b)]^{-1}$

$= e'(e')^{-1}$

$= e'.e'$

$= e'$

$\therefore f(ab^{-1}) = e'$.

$\therefore ab^{-1} \in K$.
$\therefore K$ is a subgroup of G.

Let $x \in G$

$\therefore f(xax^{-1}) = f(x)\,f(a)\,[f(x)]^{-1}$
$= f(x)\cdot e'\,[f(x)]^{-1}$
$= f(x)\,[f(x)]^{-1}$
$= e'$

$\therefore f(xax^{-1}) = e'$
$\therefore xax^{-1} \in K$.
$\therefore K$ is normal subgroup of G.

Theorem → The necessary and sufficient condition for a homomorphism f of a group G onto a group G' with Kernel K to be an isomorphism of G onto G' is that $K = \{e\}$.

(or)

If $f: G \to G'$ is a homomorphism & onto, then $\ker f = \{e\}$.
$\iff f$ is $1-1$.

proof: Let $f: G \to G'$ be a homomorphism and onto.
Let e, e' be the identity elements in G & G'.
Let K be the Kernel of f.
$\therefore K = \{x \in G \mid f(x) = e'\}$
Suppose that $f: G \to G'$ is isomorphism. then
f is $1-1$.
To prove $K = \{e\}$.
Let $a \in K$
$\therefore f(a) = e'$
$\Rightarrow f(a) = f(e)$
$\Rightarrow a = e$ ($\because f$ is $1-1$)
$\therefore e$ is the identity element in G.
which belongs to K.
$\therefore K = \{e\}$.

Converse
Suppose that $K = \{e\}$.
Let $a, b \in G$.

Now we have $f(a) = f(b)$

$\Rightarrow f(a)[f(b)]^{-1} = f(b)[f(b)]^{-1}$

$\Rightarrow f(a)f(b^{-1}) = e'$

$\Rightarrow f(ab^{-1}) = e'$

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

$\Rightarrow ab^{-1} = e$

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

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

$\Rightarrow ae = b$

$\Rightarrow a = b$

$\therefore f$ is 1-1

$\therefore f$ is an isomorphism from G to G'.

Theorem → Let f be a homomorphism from a group G onto a group G'. Let $\ker f = K$.

Let 'a' be a given element of G such that $f(a) = d \in G'$

Then the set of all those elements of G which have the image a' in G' is the coset Ka of K in G.

Proof: Let $f: G \to G'$ be homomorphism & onto.

Let e be the identity element in G and e' be the identity element in G'.

Let $\ker f = K$ then $K = \{x \in G \mid f(x) = e'\}$.

Let $a \in G$ such that $f(a) = a' \in G'$.

$f^{-1}(a') = \{x \in G \mid f(x) = a'\} = T$ (say).

Now to prove that $f^{-1}(a') = Ka$

Let $y \in Ka$. Then $y = ka$ for some $k \in K$.

$\therefore f(y) = f(ka)$

$= f(k)f(a)$

$= e'.f(a)$ $\quad (\because k \in K \Rightarrow f(k) = e')$

$= f(a)$

$= a'$

$\therefore f(y) = a'$

$\Rightarrow y \in f^{-1}(a')$.

$\therefore y \in Ka \Rightarrow y \in \bar{f}^{-1}(a')$

$\therefore Ka \subseteq \bar{f}^{-1}(a')$ —— (1)

Let $z \in \bar{f}^{-1}(a')$ then $f(z) = a'$.

Now we have

$$f(za^{-1}) = f(z)\, f(a^{-1})$$
$$= f(z)[f(a)]^{-1}$$
$$= a'(a')^{-1}$$
$$= e' \quad (\because f(a)\cdot[f(a)]^{-1} = e')$$

$\therefore f(za^{-1}) = e'$

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

$\Rightarrow (za^{-1})a \in Ka$

$\Rightarrow z \in Ka$.

$\therefore z \in \bar{f}^{-1}(a') \Rightarrow z \in Ka$

$\Rightarrow \bar{f}^{-1}(a') \subseteq Ka$ —— (2)

From (1) & (2), we have

$$\bar{f}^{-1}(a') = Ka.$$

Theorem Let G be a group and N be a normal subgroup of G. Let f be a mapping from $G \to \frac{G}{N}$ defined by $f(x) = Nx$ for $x \in G$. Then f is a homomorphism of G onto $\frac{G}{N}$ and $\ker f = N$.

Proof: Let $f: G \to \frac{G}{N}$ such that $f(x) = Nx \ \forall x \in G$.

To show f is onto:

Let $Nx \in \frac{G}{N}$ then $x \in G$.

$\therefore f(x) = Nx$.

$\therefore f$ is onto.

To show f is homomorphism:

Let $a, b \in G \Rightarrow ab \in G$.

Now we have

$$f(ab) = N(ab) \quad (ab \in G \text{ by defn})$$
$$= Na \cdot Nb \quad (\because N \text{ is normal})$$
$$= f(a)\cdot f(b)$$

$\because$ f is homomorphism from $G \to \frac{G}{N}$. and onto.

i.e, f is homomorphism of G onto $\frac{G}{N}$.

i.e, every quotient group of a group is a homomorphic image of the group.

Now to prove $\ker f = N$.

Let K be kernel of this homomorphism 'f'.

The identity of the quotient group $\frac{G}{N}$ is the coset N.

$\therefore K = \{ y \in G / f(y) = N \}$.

Let $k \in K \Leftrightarrow f(k) = N$.

$\Leftrightarrow Nk = N$ ($\because$ by defn of f. i.e, $f(x) = Nx \ \forall x \in G$)

$\Leftrightarrow k \in N$.

($\because a \in H \Leftrightarrow Ha = H$)

$\therefore K = N$.

i.e, $\ker f = N$.

Note: The mapping $f: G \to \frac{G}{N}$ such that $f(x) = Nx \ \forall x \in G$. is called Natural (or) Canonical homomorphism.

Fundamental theorem on Homomorphism of groups:

Every homomorphic image of a group G is isomorphic to some quotient group of G.

(or)

If f is a homomorphism from a group G onto a group G', then $\frac{G}{\ker f}$ (i.e, $\frac{G}{K}$) is isomorphic with G'.

(or)

If $f: G \to G'$ is a homomorphism and onto with kernel K, then prove that $\frac{G}{K} \cong G'$.

Proof: By defn of kernel f is

$K = \{ x \in G / f(x) = e' ; e' \text{ is the identity element in } G' \}$

W.K.T K is a normal subgroup of G.

$\therefore$ the quotient group $\frac{G}{K}$ is defined.

where $\frac{G}{K} = \{ Ka / a \in G \}$

Given that the mapping $f: G \to G'$ is homomorphism and onto.

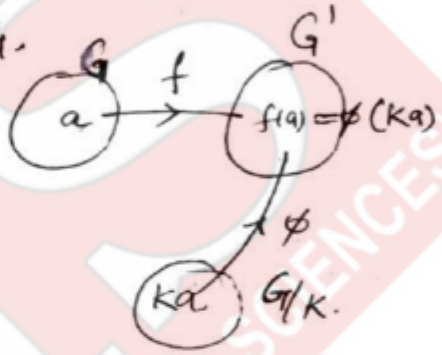
$\Rightarrow f(a) \in G' \quad \forall a \in G.$

Now we shall prove that $\frac{G}{K} \cong G'$.

i.e, G' is isomorphic image of $\frac{G}{K}$.

Define a mapping $\phi: \frac{G}{K} \to G'$ such that

$\phi(Ka) = f(a) \quad \forall a \in G.$



(i) Now we shall show that ϕ is well defined:

for $a, b \in G$; $Ka, Kb \in \frac{G}{K}$.

we have $Ka = Kb$

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

$\Rightarrow f(ab^{-1}) = e'$ where $e' \in G'$

$\Rightarrow f(a) \cdot f(b^{-1}) = e'$ ($\because f$ is homo).

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

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

$\Rightarrow f(a) f(e) = f(b)$

$\Rightarrow f(a) \cdot e' = f(b)$

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

$\Rightarrow \phi(Ka) = \phi(Kb)$ (by defn)

$\therefore \phi$ is well defined.

(ii) To prove ϕ is 1-1:

for $a, b \in G$, $Ka, Kb \in \frac{G}{K}$.

Now we have $\phi(Ka) = \phi(Kb)$

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

$\Rightarrow f(a)[f(b)]^{-1} = f(b)[f(b)]^{-1}$

$\Rightarrow f(a)\, f(b^{-1}) = e'$

$\Rightarrow f(ab^{-1}) = e'$

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

$\Rightarrow Ka = Kb$.

$\therefore \phi$ is 1-1

(iii) To prove that ϕ is onto:

Let $x \in G'$

Since $f: G \to G'$ is onto.

$\therefore \exists\ a \in G$ such that $f(a) = x$.

$\therefore Ka \in \frac{G}{K}$ and $\phi(Ka) = f(a)$ $\forall a \in G$.

$= x$.

$\therefore \phi(Ka) = x$ $\forall a \in G$.

$\therefore \phi$ is onto.

(iv) To prove ϕ is homomorphism:

for $a, b \in G$, $Ka, Kb \in \frac{G}{K}$.

Now we have

$\phi[(Ka)(Kb)] = \phi(Kab)$ ($\because K$ is normal)

$= f(ab)$ ($\because$ by defn)

$= f(a) f(b)$

$= \phi(Ka)\, \phi(Kb)$.

$\therefore \phi[(Ka)(Kb)] = \phi(Ka) \cdot \phi(Kb)$.

$\therefore \phi$ is homomorphism.

$\therefore \phi$ is an isomorphism from $\frac{G}{K}$ onto G'.

i.e, G' is an isomorphic image of $\frac{G}{K}$.

i.e, $\frac{G}{K} \cong G'$.

Problems:

→ If for a group G, $f: G \to G$ is given by $f(x) = x^2$ $\forall x \in G$. is a homomorphism, prove that G is abelian.

Sol^n: $f: G \to G$ such that $f(x) = x^2 \ \forall x \in G$.
is a homomorphism.

Let $x, y \in G \Rightarrow xy \in G$.

$\therefore f(x) = x^2$, $f(y) = y^2$, $f(xy) = (xy)^2$

Since f is homomorphism,

$f(xy) = f(x) \cdot f(y)$

$\Rightarrow (xy)^2 = x^2 y^2$

$\Rightarrow (xy)(xy) = x \cdot x \cdot y \cdot y$

$\Rightarrow x(yx)y = x(xy)y$

$\Rightarrow yx = xy$

$\therefore G$ is abelian.

→ Let G be a x^{ve} group and $f: G \to G$ such that $a \in G$, $f(a) = a^{-1}$. P.T f is 1-1 and onto. Also prove that f is homomorphism iff G is commutative.

Sol^n: $f: G \to G$ is a mapping such that $f(a) = a^{-1}$ for $a \in G$.

(i) To show f is 1-1 :-

Let $a, b \in G \Rightarrow a^{-1}, b^{-1} \in G$. and $f(a), f(b) \in G$.

Now we have

$f(a) = f(b)$

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

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

$\Rightarrow a = b$

$\therefore f$ is 1-1.

(ii) To prove f is onto:

Let $a \in G$.

$\therefore a^{-1} \in G$ such that $f(a^{-1}) = (a^{-1})^{-1} = a$

$\therefore f$ is onto.

(iii) Suppose f is a homomorphism.

for $a, b \in G \Rightarrow ab \in G$.

$\therefore f(a) = a^{-1}$, $f(b) = b^{-1}$ and $f(ab) = (ab)^{-1}$

Since f is homomorphism.

$\therefore f(ab) = f(a) \cdot f(b)$

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

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

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

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

$\Rightarrow ab = ba$.

$\therefore G$ is abelian.

Suppose G is abelian.

for $a, b \in G$

Now we have

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

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

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

$= f(a)\, f(b)$

$\therefore f$ is homomorphism.

→ If $f: G \to G'$ is defined by $f(x) = 1$; $x > 0$

$= -1$; $x < 0$.

where G = set of non-zero real numbers and

$G' = \{1, -1\}$ are groups.

Prove that f is a homomorphism. and find kernel.

Sol^n: Clearly $G = \mathbb{R} - \{0\}$.

$G' = \{1, -1\}$ are groups w.r.t x^n.

and identity in G' is 1.

Let $x, y \in G$ then $f(x), f(y) \in G'$.

(i) Let $x > 0$, $y > 0$

$\Rightarrow xy > 0$

$\therefore f(x) = 1$, $f(y) = 1$ & $f(xy) = 1$

Now $f(xy) = 1 = 1 \cdot 1 = f(x) \cdot f(y)$.

(ii) Let $x<0$, $y<0$

$\Rightarrow xy>0$

$\therefore f(x)=-1$, $f(y)=-1$ and $f(xy)=1$

Now $f(xy)=1$

$=(-1)(-1)$

$=f(x)\,f(y)$

(iii) Let $x>0$, $y<0$ (or $x<0$, $y>0$)

$\Rightarrow xy<0$

$\therefore f(x)=1$, $f(y)=-1$ & $f(xy)=-1$

Now $f(xy)=-1$

$=(1)(-1)$

$=f(x)\,f(y)$

$\therefore$ from (i), (ii), (iii)

we have

$\forall x, y \in G$

$f(xy)=f(x)\,f(y)$

$\therefore f$ is homomorphism from $G \to G'$.

Kernel $f=\{x\in G / f(x)=1,$ identity in $G'\}$.

$=\{x\in G / x>0\}$.

→ Let $(G,+)$ is a group of real number and $(G',\cdot)$ is a group of +ve real numbers. Let $f: G\to G'$ be a mapping such that $f(x)=e^x$ for $x\in G$. Show that f is an isomorphism & onto.

Soln: If x is a real number, $e^x>0$ and hence $e^x\in G'$.

Let $a, b\in G$

$\therefore e^a, e^b \in G'$.

i.e, $f(a)=e^a$ & $f(b)=e^b$.

Now we have $f(a)=f(b)$

$\Rightarrow e^a=e^b$.

$\Rightarrow a = b$

$\therefore f$ is 1-1.

Let $c \in G'$

i.e, c is a +ve real number and $\log c$ is real number. (+ve or -ve or zero).

Also $\log c \in G$.

$\therefore f(\log c) = e^{\log c}$ (by defn)

$= c$

$\therefore \exists \log c \in G$ such that $f(\log c) = c$.

$\therefore f$ is onto.

Let $a, b \in G \Rightarrow a+b \in G$.

$\therefore f(a) = e^a$, $f(b) = e^b$ & $f(a+b) = e^{a+b}$.

Now we have

$f(a+b) = e^{a+b}$

$= e^a \cdot e^b$.

$= f(a)\, f(b)$

$\therefore f$ is homomorphism, which is 1-1 & onto.

$\therefore f$ is an isomorphism.

→ If 'f' is a homomorphism of G onto G' and 'g' is homomorphism of G' onto G'', show that gof is a homomorphism of G onto G''

Also show that the kernel of f is a subgroup of the kernel of gof.

Soln: $f: G \to G'$ is a homomorphism & onto.

$g: G' \to G''$ is a homomorphism & onto.

$\therefore gof: G \to G''$ is a mapping of G onto G'' such that $(gof)(x) = g(f(x))$ $\forall x \in G$.

Let $a, b \in G$

Then $(gof)(ab) = g[f(ab)]$

$= g[f(a) \cdot f(b)]$. ($\because f$ is homo.)

$= g(f(a)) \cdot g(f(b))$ ($\because$ g is homo).

$= (gof)(a) \cdot (gof)(b)$.

$\therefore$ gof is homomorphism from G onto G''.

Let e' be identity element in G'.

If K' be the kernel of f

then $K' = \{ x \in G / f(x) = e' \}$.

Let e'' be the identity element in G''.

If K'' be the kernel of gof.

then $K'' = \{ y \in G / (g \circ f)(y) = e'' \}$.

TO show that the kernel of f is a subgroup of the kernel of gof.

i.e, to show that $K' \subseteq K''$

Let $k' \in K'$ then $f(k') = e'$.

Also $k' \in G$.

Now $(gof)(k') = g(f(k'))$

$= g(e')$

$= e''$ ($\because$ g is hom).

$\therefore k' \in K''$

$\therefore k' \in K' \Rightarrow k' \in K''$.

$\therefore K' \subseteq K''$

Theorem

Let $f: G \to G'$ be a homomorphism.

If the order of $a \in G$ is finite then the order of f(a) is a divisor of the order of a.

i.e, $\frac{o(a)}{o(f(a))}$.

Proof: Let $a \in G$ and $o(a) = m$ then $a^m = e$. where m is the least +ve integer.

$\therefore f(a^m) = f(e)$

$\Rightarrow f[a.a.....a \text{ (m times)}] = e'$.

$\Rightarrow f(a)\cdot f(a)\cdots\cdots$ m times $= e'$ ($\because$ f is homo).

$\Rightarrow [f(a)]^m = e'$.

$\therefore$ If 'n' is the order of f(a) in G', then 'n' must be a divisor of 'm'.

($\because$ If the element 'a' of a group G is of order 'n' then $a^m = e \Leftrightarrow$ n is a divisor of m).

Theorem 2005

If $f: G \to G'$ is an isomorphism (i.e, o(f(a)) divides order of 'a', $a \in G$), then the order of $a \in G$ is equal to the order of its image f(a).

Proof: Let $o(a) = n$; $a \in G$ then $a^n = e$, where n is the least +ve integer.

$\therefore f(a^n) = f(e)$

$\Rightarrow f(a\cdot a\cdots\cdots n \text{ times}) = f(e)$

$\Rightarrow f(a)\cdot f(a)\cdots\cdots n \text{ times} = f(e)$ ($\because$ f is homo).

$\Rightarrow [f(a)]^n = f(e) = e'$ where e' is identity in G'.

$\Rightarrow o[f(a)] \le n$ ——— ①

Let $o[f(a)] = m$ then

$[f(a)]^m = e'$. where m is the least +ve integer

$\Rightarrow f(a)\cdot f(a)\cdots\cdots m \text{ times} = e'$

$\Rightarrow f(a\cdot a\cdots\cdots m \text{ times}) = f(e)$

$\Rightarrow f(a^m) = f(e)$

$\Rightarrow a^m = e$ ($\because$ f is 1-1)

$\Rightarrow o(a) \le m$ ——— ②

from ① & ② we have

$m \le n$ & $n \le m$.

$\Rightarrow m = n$

$\Rightarrow o[f(a)] = o(a)$.

Note: 1 If the order of 'a' is finite then the order of f(a) cannot be finite. Because if the order of f(a) is finite and is equal to 'm'. (i.e, $O(f(a)) = m$), then $a^m = e$.

$\therefore O(a)$ is finite

which is a contradiction.

2. Let f be an isomorphic mapping of a group G into a group G'. then

(i) the f-image of the identity element 'e' of G is the identity element e' of G'.

i.e, $f(e) = e'$.

(ii) The f-image of the inverse of an element 'a' of G is the inverse of the f-image of a.

i.e, $f(a^{-1}) = [f(a)]^{-1}$.

(iii) The order of an element 'a' of G is equal to the order of its image. f(a).

i.e, $O(a) = o(f(a))$.

3. Suppose we are to prove that a group G is isomorphic to another group G', then we should try to find a 1-1 mapping from G onto G' which also preserves compositions in G and G'. while forming such a mapping we should keep in mind the above three facts (i.e, in Note 2) that an isomorphic mapping must preserve identities, inverses and orders.

Problems

1. → Show that the group $(G = \{0, 1, 2, 3\}, +_4)$ and the group $(G' = \{1, -1, i, -i\}, \cdot)$ are isomorphic.

Sol^n: Here 0 is the identity element in G and 1 is the identity element in G'

$\therefore$ If f is isomorphism of G onto G' then $f(0)=1$ (i.e, f

In G, the orders of $1, 2, 3$ are $4, 2$ and 4 respectively

In G', the orders of $-1, i, -i$ are $2, 4$ and 4 respectively

W.k.T in isomorphic mapping only elements of equal order can be mapped on each other

$\therefore f(2) = -1$ and $f(1) = i$ or $-i$ & $f(3) = i$ or $-i$.

Let $f(1) = i$ and $f(3) = -i$.

Now we observe that $f(a^{-1}) = [f(a)]^{-1}$ for $a \in G$.

Since $f(i^{-1}) = f(3) = -i$

$= i^{-1}$.

$\therefore f(i^{-1}) = [f(1)]^{-1}$

$f(2^{-1}) = f(2)$

$= -1$

$= -1^{-1}$

$= [f(2)]^{-1}$

Similarly $f(3^{-1}) = [f(3)]^{-1}$

$\therefore$ The mapping $f: G \to G'$ is $1-1$ and onto.

To Show f is homomorphism:

Now we form the composition tables for G & G'.

$(G, +_4)$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$(G, \cdot)$

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

for $a, b \in G$

$f(a +_4 b) = f(a) \cdot f(b)$.

Since $f(0 +_4 2) = f(2)$

$= -1$.

and $f(0) \cdot f(3) = 1(-1) = -1$.

$\therefore f(0 +_4 2) = f(0) \cdot f(2)$ etc.

$\therefore f$ is homomorphism.

Also f is 1–1 & onto.

$\therefore f$ is an isomorphism of G onto G'.

Hence G' is isomorphic image of G.

Note: The $\phi : G \to G'$ defined $\phi(0) = 1$, $\phi(2) = -1$, $\phi(1) = -i$ and $\phi(3) = i$ is also an isomorphism of G onto G'. In this case we have only two isomorphisms of G onto G'.

H.W → Show that the multiplicative group $G = \{1, -1, i, -i\}$ is isomorphic to the permutation group $G' = \{I, (a\,b\,c\,d), (a\,c)(b\,d), (a\,d\,c\,b)\}$ on four symbols a, b, c, d.

H.W. → Show that the x^ve group $G = \{1, \omega, \omega^2\}$ is isomorphic to the permutation group $G' = \{I, (a\,b\,c), (a\,c\,b)\}$ on three symbols a, b, c.

→ Show that the mapping $f : G \to G'$ such that $f(x+iy) = x$ where G is a group of complex numbers under $+^n$, G' is a group of real numbers under $+^n$ is a homomorphism onto and find kerf.

Sol^n: Let $a = a_1 + ib_1$, $b = a_2 + ib_2 \in G$.

$\Rightarrow a + b \in G$.

$\therefore f(a) = f(a_1 + ib_1) = a_1$

and $f(b) = f(a_2 + ib_2) = a_2$

Now $f(a+b) = f\left((a_1 + ib_1) + (a_2 + ib_2)\right)$

$= f\left((a_1 + a_2) + i(b_1 + b_2)\right)$

$= a_1 + a_2$ (by defn)

$= f(a)+f(b)$

$\therefore f$ is a homomorphism.

Let $c \in G'$ where c is a real number.

and $c+iy \in G$.

so that $f(c+iy) = c$ for $y \in \mathbb{R}$.

$\therefore f$ is onto.

$\therefore f$ is a homomorphism from G onto G'.

The identity in G' is 0.

Since $\ker f = \{x+iy \in G / f(x+iy) = x = 0\}$.

$\ker f = \{0+iy / y \in \mathbb{R}\}$.

→ Show that the mapping $f: G \to G'$ such that $f(z) = |z|$, for $z \in G$. where G is a multiplicative group of non-zero complex numbers and G' is a x^{ve} group of non-zero real numbers is a homomorphism. find $\ker f$.

Sol^n: Let $z_1, z_2 \in G$.

$\therefore f(z_1) = |z_1|$

$f(z_2) = |z_2|$.

Now we have

$f(z_1 z_2) = |z_1 z_2|$

$= |z_1|\,|z_2|$

$= f(z_1)\, f(z_2)$.

$\therefore f$ is homomorphism.

The identity in G' is 1.

$\therefore \ker f = \{a+ib \in G / f(a+ib) = (a+ib) = \sqrt{a^2+b^2} = 1\}$.

Theorem: If H and N are subgroups of a group G and N is normal subgroup of G. then $\frac{HN}{N} \cong \frac{H}{H \cap N}$.

proof: Since H & N subgroups of G.

and N is a normal subgroup of G.

$\therefore HN$ is a normal subgroup of H.

Also HN is a subgroup of G and $N \subseteq HN$.

Since N is normal in G.

$\therefore N$ is normal subgroup of HN.

$\therefore$ The quotient groups $\frac{HN}{N}$ & $\frac{H}{H \cap N}$ are defined.

Now we define

$\phi : H \to \frac{HN}{N}$ such that

$\phi(x) = Nx \quad \forall x \in H$ ——— (1) ($\because N \subseteq HN$, $x \in H \Rightarrow x \in HN$. $\therefore Nx \in \frac{HN}{N}$)

To show ϕ is well defined:

$x_1, x_2 \in H$

we have $x_1 = x_2$

$\Rightarrow Nx_1 = Nx_2$

$\Rightarrow \phi(x_1) = \phi(x_2)$

$\therefore \phi$ is well defined.

To show ϕ is homomorphism:

Let $x_1, x_2 \in H$, $Nx_1, Nx_2 \in \frac{HN}{N}$.

then $\phi(x_1) = Nx_1$ & $\phi(x_2) = Nx_2$ (by (1))

Now we have

$\phi(x_1 \cdot x_2) = N(x_1 \cdot x_2)$ (by (1))

$= Nx_1 \cdot Nx_2$

$= \phi(x_1)\,\phi(x_2)$. ($\because N$ is normal in HN.)

$\therefore \phi$ is homomorphism

To show ϕ is onto:

Let $x \in \frac{HN}{N}$

then $x = Ng$ for some $g \in HN$.

Now $g \in HN \Rightarrow g = hn$ for some $h \in H, n \in N$.

Since N is normal in G.

$\therefore HN = NH$.

$\therefore \exists\ n' \in N,\ h' \in H$ such that $hn = n'h'$.

we have $\phi(h') = Nh'$

$= (Nn')h'$ $(\because n' \in N \Rightarrow Nn' = N)$

$= N(n'h')$

$= N(hn) = Ng$.

$\therefore Ng \in \frac{HN}{N} \Rightarrow \exists\ h' \in H$ such that $\phi(h') = Ng$

$\therefore \phi$ is onto.

$\therefore \phi$ is homomorphism of H onto $\frac{HN}{N}$.

Since $\phi : H \to \frac{HN}{N}$ is homomorphism and onto

$\therefore$ By fundamental theorem of homomorphism,

we have $\frac{H}{\ker\phi} \cong \frac{HN}{N}$ ——— (2)

$f: G \to G'$ homo & onto
$\phi: \frac{G}{K} \to G'$
$\frac{G}{K} \cong G'$

Now to show that the kernel of $\phi = H \cap N$

Now $\ker\phi = \{x \in H / \phi(x) = N\}$ where N is the identity in $\frac{HN}{N}$

Let $x \in \ker\phi$.

$\Leftrightarrow \phi(x) = N$ and $x \in H$

$\Leftrightarrow Nx = N$ and $x \in H$

$\Leftrightarrow x \in N$ $(\because N$ is normal in $G)$ and $x \in H$.

$\Leftrightarrow x \in H \cap N$.

$\therefore \ker\phi = H \cap N$. ——— (3)

from (2) & (3)

$$\frac{H}{H \cap N} \cong \frac{HN}{N}$$

Hence $\frac{HN}{N} \cong \frac{H}{H \cap N}$

Homomorphisms of Groups

Up till now we were concerned only with a group and its substructure, and observed several important algebraic features of this fundamental structure. In this chapter, we are going to examine the interplay between algebraic properties of two groups by defining some suitable functions between them. This idea will lead us towards the concept of *homomorphism*, which in a sense, establishes a structural compatibility between two algebraic structures. Gradually it enables us to develop the key concept of *isomorphism* among algebraic structures— in particular, groups. Two isomorphic algebraic structures can be regarded, for all practical purposes, to be algebraically similar, in the sense that they share precisely the same algebraic characters. That is why the concept of ispmorphism plays the central role in classification of different algebraic structures.

Homomorphisms

Let us begin our discussion by considering the groups $(\mathbb{R}, +)$ and $(\mathbb{R}^+, \cdot)$, where the first one is the group of all real numbers under addition and the other one is the group of all positive real numbers under multiplication. Define a function $h : \mathbb{R} \to \mathbb{R}^+$ by $h(a) = e^a$ for all $a \in \mathbb{R}$. Observe that

$$h(a + b) = e^{a+b} = e^a \cdot e^b = h(a) \cdot h(b) \text{ for all } a, b \in \mathbb{R}.$$

So we see that the above function establishes an interesting relation between the operations of two groups under discussion. In this example, note that $a, b \in \mathbb{R}$, whence $a + b \in \mathbb{R}$. Now $h(a)$ and $h(b)$ are elements of $\mathbb{R}^+$ and so is $h(a) \cdot h(b)$. Now $h(a + b) \in \mathbb{R}^+$ and also satisfies $h(a + b) = h(a)\ h(b)$. Obviously, any arbitrary

function between two groups do not necessarily enjoy this kind of property. In the sequel, functions of this special type between two groups will establish a relation between two groups.

Definition 6.1.1. Let $(G, *)$ and $(G_1, *_1)$ be two groups and f be a function from G into G_1. Then f is called a *homomorphism* of G into G_1 if for all $a, b \in G$,

$$f(a * b) = f(a) *_1 f(b).$$

Observe that the above defined function $h : \mathbb{R} \to \mathbb{R}^+$ is an example of a homomorphism from the group $(\mathbb{R}, +)$ to the group $(\mathbb{R}^+, \cdot)$.

We now consider some examples to explain the notion of homomorphism of groups.

Example 6.1.2. Consider the groups $(\mathbb{Z}, +)$, the group of all integers under addition and the multiplicative group $(\{1, -1\}, \cdot)$. Define $f : \mathbb{Z} \to \{1, -1\}$ by

$$f(n) = 1, \text{ if } n \text{ is an even integer;}$$

$$= -1, \text{ if } n \text{ is an odd integer.}$$

Let $n, m \in \mathbb{Z}$. If n, m are both even, then $n + m$ is even and hence $f(n + m) = 1 = 1 \cdot 1 = f(n) \cdot f(m)$. Suppose n is even and m is odd, then $n + m$ is odd. Then $f(n) = 1, f(m) = -1$ and $f(n + m) = -1 = 1 \cdot (-1) = f(n) \cdot f(m)$. Similar is the situation, when m is even and n is odd. Now, when both n and m are odd, we see that $n + m$ is even, whence $f(n + m) = 1 = (-1) \cdot (-1) = f(n)\, f(m)$. Combining all these cases, we find that for any two integers n, m, $f(n + m) = f(n) \cdot f(m)$. Hence f is a homomorphism from the group $(\mathbb{Z}, +)$ to the group $(\{1, -1\}, \cdot)$.

Example 6.1.3. Let $(G, *)$ and $(G_1, *_1)$ be two groups. Let the identity element of the group $(G_1, *_1)$ be e_1. Define $f : G \to G_1$ by $f(a) = e_1$ for all $a \in G$. Since $f(a * b) = e_1 = e_1 *_1 e_1 = f(a) *_1 f(b)$ for all $a, b \in G$, we find that f is a homomorphism.

This example shows that between any two groups there always exists a homomorphism. This homomorphism is called the *trivial homomorphism*.

Example 6.1.4. Consider the group $GL(2, \mathbb{R})$ of all 2×2 nonsingular matrices under matrix multiplication and the group R^* of all nonzero real numbers under usual multiplication. Define $f : GL(2, \mathbb{R}) \to \mathbb{R}^*$ by $f(A) = det\, A$ for all $A \in GL(2, \mathbb{R})$,

where $det\, A$ means the determinant value of the nonsingular square matrix A. Let $A, B \in GL(2, \mathbb{R})$. Hence $det\, A, det\, B \in R^*$. Now $AB \in GL(2, \mathbb{R})$ and we know that $det\, AB = det\, A\, det\, B$. Hence,

$$f(AB) = det\,(AB) = det\, A\, det\, B = f(A)f(B).$$

So it follows that f is a homomorphism.

Example 6.1.5. Consider the group $(\mathbb{Z}, +)$. Define $f : \mathbb{Z} \to \mathbb{Z}$ by $f(n) = n + 1$. This is a function from $\mathbb{Z}$ to $\mathbb{Z}$. But for this function,

$$f(2+5) = f(7) = 7 + 1 = 8 \neq 9 = (2+1) + (5+1) = f(2) + f(5).$$

Hence this function f is *not* a *homomorphism* from the group $(\mathbb{Z}, +)$ to itself.

Suppose on the same group, f is defined by $f(n) = 3n$ for all $n \in \mathbb{Z}$. Let $n, m \in \mathbb{Z}$, then $n + m \in \mathbb{Z}$ and we have

$$f(n+m) = 3(n+m) = 3n + 3m = f(n) + f(m).$$

Hence the function f is a homomorphism.

The reader will shortly realize that one of the most useful tools in the group theory is the idea of homomorphism of groups. Indeed, the fact that there exists a homomorphism of groups $f : G \to G_1$ helps us to draw some conclusion about the nature of G_1 from the nature of G.

From the definition of homomorphism f of groups, we have seen that f preserves group operations. In the following theorem, we show that f also preserves identities and inverses.

Theorem 6.1.6. *If f is a homomorphism from a group G into a group G_1 and e, e_1 are the identity elements of G and G_1 respectively, then*

(i) $f(e) = e_1$.

(ii) $f(a^{-1}) = f(a)^{-1}$ *for all* $a \in G$.

(iii) $f(a^n) = f(a)^n$ *for all* $a \in G$ *and for all* $n \in \mathbb{Z}$. [We denote $\big(f(a)\big)^n$ by $f(a)^n$].

Proof. (i) By the definition of homomorphism, $f(e) = f(ee) = f(e)f(e)$. Since $f(e) \in G_1$, $f(e) = f(e)e_1$. Hence $f(e)e_1 = f(e)f(e)$. By the cancellation property, we find that $f(e) = e_1$.

(ii) Let $a \in G$. Then $f(a)f(a^{-1}) = f(aa^{-1}) = f(e) = e_1$ (by (i)). Similarly, $f(a^{-1})f(a) = f(a^{-1}a) = f(e) = e_1$. Hence $f(a^{-1})$ is an inverse of $f(a)$ in G_1, and as inverse of an element in a group is unique, we have $f(a^{-1}) = f(a)^{-1}$.

(iii) We first prove that $f(a^n) = f(a)^n$ for all $n \geq 0$. For $n = 0$, the result follows from (i). If $n = 1$, then $f(a) = f(a)$. Suppose $f(a^k) = f(a)^k$ for some positive integer k. Now,

$$\begin{aligned} f(a^{k+1}) &= f(a^k a) \\ &= f(a^k)f(a) \quad \text{(since } f \text{ is a homomorphism)} \\ &= f(a)^k f(a) \quad \text{(by induction hypothesis)} \\ &= f(a)^{k+1} \end{aligned}$$

Hence by induction, $f(a^n) = f(a)^n$ for $n \geq 1$.

Now suppose that $n = -m$, where for $m > 0$. Then,

$$\begin{aligned} f(a^n) &= f(a^{-m}) \\ &= f\left((a^{-1})^m\right) \\ &= f(a^{-1})^m \quad \text{(since } m > 0) \\ &= \left(f(a)^{-1}\right)^m \quad \text{(by (ii))} \\ &= f(a)^{-m} \\ &= f(a)^n. \end{aligned}$$

□

Observe that the function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = n + 1$ in the Example 6.1.5 above, is not a homomorphism, follows from the last theorem also, since $f(0) = 0 + 1 = 1$, which is not the identity element of $(\mathbb{Z}, +)$.

We now prove some other basic properties of homomorphism.

Theorem 6.1.7. *Let f be a homomorphism of a group G into a group G_1. Then the following results hold:*

(i) if H is a subgroup of G, then $f(H) = \{f(h) \mid h \in H\}$ is a subgroup of G_1;

(ii) if H_1 is a subgroup of G_1, then $f^{-1}(H_1) = \{g \in G \mid f(g) \in H_1\}$ is a subgroup of G and if H_1 is a normal subgroup, then $f^{-1}(H_1)$ is a normal subgroup of G;

(iii) if $a \in G$ is such that $o(a) = n$, then $o\left(f(a)\right)$ divides n.

Proof. (i) Let H be a subgroup of G. Then $e \in H$ and by Theorem 6.1.6 (i), $f(e) = e_1$, where e_1 is the identity of G_1. Thus, $e_1 = f(e) \in f(H)$ and so $f(H) \neq \emptyset$.

Let $x, y \in f(H)$. Then there exist a, b in H such that $f(a) = x, f(b) = y$. Since H is a subgroup, $ab^{-1} \in H$ and so $xy^{-1} = f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1}) \in f(H)$. Hence, by Theorem 5.1.5, $f(H)$ is a subgroup of G_1.

(ii) Since $e_1 \in H_1$ and $f(e) = e_1$, we find that $e \in f^{-1}(H_1)$ and so $f^{-1}(H_1) \neq \emptyset$. Let $a, b \in f^{-1}(H)$. Then $f(a), f(b) \in H_1$. Hence, $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} \in H_1$ and so $ab^{-1} \in f^{-1}(H_1)$. Then by Theorem 5.1.5, $f^{-1}(H_1)$ is a subgroup of G. Suppose now, that H_1 is a normal subgroup of G_1. Let $g \in G$. We now show that $gf^{-1}(H_1)g^{-1} \subseteq f^{-1}(H_1)$. Let $a \in gf^{-1}(H_1)g^{-1}$. Then $a = gbg^{-1}$ for some $b \in f^{-1}(H_1)$. Now $f(a) = f(gbg^{-1}) = f(g)f(b)f(g^{-1}) = f(g)f(b)f(g)^{-1} \in H_1$, since $f(g) \in G_1, f(b) \in H_1$ and H_1 is a normal subgroup in G_1. Hence $a \in f^{-1}(H_1)$ and this shows that $gf^{-1}(H_1)g^{-1} \subseteq f^{-1}(H_1)$. Thus, $f^{-1}(H_1)$ is a normal subgroup of G.

(iii) Since $f(a)^n = f(a^n) = f(e) = e_1$, we have $o\big(f(a)\big)$ divides n, by Theorem 6.1.19(i). □

Before proceeding further, we consider another example of homomorphism of groups.

Example 6.1.8. Let $\mathbb{R}^+$ denote the group of all positive real numbers under multiplication and $\mathbb{C}^*$ denote the group of all nonzero complex numbers under usual multiplication. Define a function $f : \mathbb{C}^* \to \mathbb{R}^+$ by $f(a + ib) = |a + ib|^2 = a^2 + b^2$. Since $a + ib \neq 0$, both a and b cannot be zero simultaneously. Hence $a^2 + b^2 \neq 0$, whence $a^2 + b^2 \in \mathbb{R}^+$. Let $u = a + ib$ and $v = c + id$ be two elements of $\mathbb{C}^*$. Then $a^2 + b^2 \neq 0$ and $c^2 + d^2 \neq 0$. Now,

$$\begin{aligned} f(uv) &= f\big((a + ib)(c + id)\big) \\ &= f\big((ac - bd) + i(ad + bc)\big) \\ &= (ac - bd)^2 + (ad + bc)^2 \\ &= a^2c^2 + b^2d^2 + c^2d^2 + b^2c^2 \\ &= (a^2 + b^2)(c^2 + d^2) \\ &= f(u)f(v). \end{aligned}$$

Hence f is a homomorphism. Now $H_1 = \{1\}$ is a subgroup of $\mathbb{R}^+$. Then,

$$\begin{aligned} f^{-1}(H_1) &= \{z \in \mathbb{C}^* \mid f(z) \in H_1\} \\ &= \{z \in \mathbb{C}^* \mid f(z) = 1\} \\ &= \{z = a + ib \in \mathbb{C}^* \mid a^2 + b^2 = 1\}. \end{aligned}$$

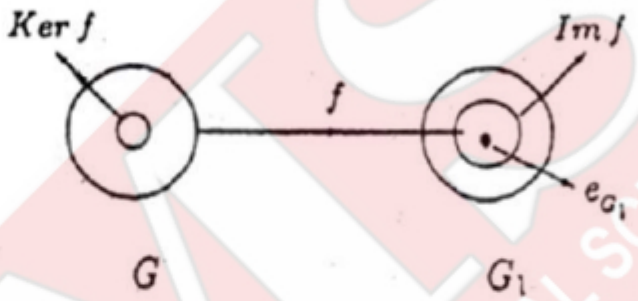
which is known to be a subgroup of $\mathbb{C}^*$.

Let $f : G \to G_1$ be a homomorphism of groups. Then one may associate, in a natural way, two subsets with f. One of these is the *image* of f, viz.,

$$Im\, f = \{f(x) \in G_1 \mid x \in G\}$$

and the other is the *kernel* of f, i.e., the set

$$Ker\, f = \{x \in G \mid f(x) = e_{G_1};\ \text{the identity element of } G_1\}.$$



Theorem 6.1.9. *Let G and G_1 be two groups and $f : G \to G_1$ be a group homomorphism. Then,*

(i) $Im\, f$ is a subgroup of G_1;

(ii) $Ker\, f$ is a normal subgroup of G.

Proof. [1] (i) Clearly $Im\, f \neq \emptyset$. Let $a, b \in Im\, f$. There exist $x, y \in G$ such that $f(x) = a$ and $f(y) = b$. Now $x^{-1}y \in G$ and $f(x^{-1}y) \in Im\, f$. But $f(x^{-1}y) = f(x^{-1})f(y) = f(x)^{-1}f(y) = a^{-1}b$. Hence $a^{-1}b \in Im\, f$ and so $Im\, f$ is a subgroup of G.

(ii) Let e_1 be the identity element of the group G_1. Then $Ker\, f = \{x \in G \mid f(x) = e_1\}$. Since $f(e) = e_1$, it follows that $e \in Ker\, f$. Hence $Ker\, f \neq \emptyset$. Let $a, b \in Ker\, f$. Then $f(a) = e_1, f(b) = e_1$ and hence $f(ab^{-1}) = f(a)f(b)^{-1} = e_1 e_1^{-1} = e_1 e_1 = e_1$. This implies that $ab^{-1} \in Ker\, f$, whence $Ker\, f$ is a subgroup of G. To show that $Ker\, f$ is a normal subgroup, let $a \in Ker\, f$ and $g \in G$; then $f(gag^{-1}) = f(g)f(a)f(g^{-1}) = f(g)e_1 f(g^{-1}) = f(g)f(g)^{-1} = e_1$ and hence $gag^{-1} \in Ker\, f$. Consequently, $Ker\, f$ is a normal subgroup of G. □

Let us now find the kernels of some of the homomorphisms already discussed in the various examples of this section.

[1] Though the proof follows from Theorem 6.1.7(i), we prefer to give a detailed proof here.

In Example 6.1.2,

$ker\, f = \{a \in \mathbb{Z} \mid f(a) = 1\} = \{2n \mid n \in \mathbb{Z}\}$,

$Im\, f = \{f(a) \mid a \in \mathbb{Z}\} = \{1, -1\}$.

In Example 6.1.3,

$ker\, f = \{a \in G \mid f(a) = e_1\} = G$;

$Im\, f = \{f(a) \mid a \in G\} = \{e_1\}$.

In Example 6.1.4,

$ker\, f = \{A \in GL(2, \mathbb{R}) \mid f(A) = 1\} = \{A \in GL(2, \mathbb{R}) \mid det\, A = 1\}$

$= SL(2, \mathbb{R})$,

$Im\, f = \{f(A) \mid A \in GL(2, \mathbb{R})\} = \{det\, A \mid A \in GL(2, \mathbb{R})\} = \mathbb{R}^*$.

In Example 6.1.5, (*Second part*)

$ker\, f = \{n \in \mathbb{Z} \mid f(n) = 0\} = \{n \in \mathbb{Z} \mid 3n = 0\} = \{0\}$,

$Im\, f = \{f(n) \mid n \in \mathbb{Z}\} = \{3n \mid n \in \mathbb{Z}\} = 3\mathbb{Z}$.

In Example 6.1.8,

$ker\, f = \{a + ib \in \mathbb{C}^* \mid f(a + ib) = 1\} = \{a + ib \in \mathbb{C}^* \mid a^2 + b^2 = 1\}$

$= \{z \in \mathbb{C}^* \mid |z| = 1\}$,

$Im\, f = \{f(a + ib) \mid a + ib \in \mathbb{C}^*\} = \{a^2 + b^2 \mid a + ib \in C^*\} = \mathbb{R}^+$.

Definition 6.1.10. Let G and G_1 be two groups and $f : G \to G_1$ be a homomorphism of groups.

(i) f is called a *monomorphism*, if f is an injective function.

(ii) f is called an *epimorphism*, if f is a surjective function

The homomorphism of Example 6.1.2 is not a monomorphism, since $f(2) = 1 = f(4)$ implies that f is not injective. However for this homomorphism $Im\, f = \{1, -1\}$, whence f is surjective and so f is an epimorphism.

Now consider the homomorphism of Example 6.1.5. Here f is an injective function. Hence f is a monomorphism. For this f, $Im\, f = 3\mathbb{Z} \neq \mathbb{Z}$ implies that f is not surjective and hence f is not an epimorphism.

Theorem 6.1.11. *A homomorphism $f : G \to G_1$ of groups is a monomorphism if and only if $Ker\, f = \{e\}$.*

Proof. Suppose f is a monomorphism. Then f is injective. Let $a \in Ker\, f$. Now $f(a) = e_1 = f(e)$, where e_1 is the identity element of G_1 and e is the identity element of G. Since f is injective, $a = e$. Hence $Ker\, f = \{e\}$.

Conversely, suppose that $Ker\, f = \{e\}$. Let $x, y \in G$ such that $f(x) = f(y)$. Then $f(x)f(y)^{-1} = e_1$, i.e., $f(x)f(y^{-1}) = e_1$, i.e., $f(xy^{-1}) = e_1$. Hence $xy^{-1} \in Ker\, f = \{e\}$ and so $xy^{-1} = e$. Consequently, $x = y$ Therefore f is injective and so f is a monomorphism. □

We shall frequently use this theorem to test whether a homomorphism f is a monomorphism or not, i.e., whether or not f is injective. For example, by virtue of this theorem also, we can say that the homomorphism f of Example 6.1.5 is a monomorphism.

Definition 6.1.12. A group G_1 is called a ***homomorphic image*** of a group G if there exists an epimorphism f from the group G onto the group G_1.

Consider the homomorphisms discussed in Example 6.1.2 and Example 6.1.4. These homomorphisms are epimorphisms. Hence the group $\{1, -1\}$ is a homomorphic image of the group $\mathbb{Z}$ and the group $\mathbb{R}^*$ is a homomorphic image of $GL(2, \mathbb{R})$. It is interesting to note that the homomorphic image of an infinite group may be a finite group.

Let us now establish the following important results.

Theorem 6.1.13. *Let G and G_1 be two groups such that G_1 is a homomorphic image of G.*

(i) If G is a commutative group, then so is G_1.

(ii) If G is a cyclic group, then so is G_1.

Proof. Since G_1 is a homomorphic image of G, there exists a homomorphism $f : G \to G_1$ of groups, such that $Im\, f = G_1$, i.e., $f(G) = \{f(x) \mid x \in G\} = G_1$.

(i) Suppose G is commutative. Let $a, b \in G_1 = f(G)$. Then there exist $x, y \in G$ such that $f(x) = a$ and $f(y) = b$. Now $ab = f(x)f(y) = f(xy) = f(yx) = f(y)f(x) = ba$. Hence G_1 is a commutative group.

(ii) Suppose G is cyclic. Let $G = \langle a \rangle$. Then $f(a) \in G_1$. Let $b = f(a)$. We show that $G_1 = \langle b \rangle$. Let $u \in G_1 = f(G)$. There exists $y \in G$ such that $f(y) = u$. Now $y \in \langle a \rangle$. Hence $y = a^n$ for some $n \in \mathbb{Z}$. Then $u = f(y) = f(a^n) = f(a)^n = b^n \in \langle b \rangle$. Consequently, $G_1 = \langle b \rangle$. □

Finding all homomorphic images of a given group is an interesting problem. We will now discuss this problem in brief.

Definition 6.1.14. A homomorphism f from a group G to a group G_1 is called an *isomorphism* if the function $f : G \to G_1$ is a bijective function. A group G_1 is said to be isomorphic to a group G, if there exists an isomorphism from G onto G_1. In this case we write $G \simeq G_1$.

Example 6.1.15. Let $(\mathbb{R}, +)$ be the group of real numbers under addition and $(\mathbb{R}^+, \cdot)$ be the group of positive real numbers under multiplication. Define $f : \mathbb{R} \to \mathbb{R}^+$ by $f(a) = e^a$ for all $a \in \mathbb{R}$. Clearly f is well-defined. We have already seen at the beginning of this section that $f(a+b) = f(a)f(b)$, whence f is a homomorphism. Suppose $f(a) = f(b)$. Then $e^a = e^b$. This implies that $a = b$, whence f is one-one. Let $b \in \mathbb{R}^+$. Then $\log_e b \in \mathbb{R}$ and $f(\log_e b) = e^{\log_e b} = b$. Thus f is onto $\mathbb{R}^+$. Consequently, f is an isomorphism of $(\mathbb{R}, +)$ onto $(\mathbb{R}^+, \cdot)$.

In the following theorem, we enlist some basic properties of isomorphisms, which shall be used to test whether a given group is isomorphic to another group or not.

Theorem 6.1.16. *Let f be an isomorphism of a group G onto a group G_1. Then,*

(i) $f^{-1} : G_1 \to G$ is an isomorphism.

(ii) G is commutative if and only if G_1 is commutative.

(iii) G is cyclic if and only if G_1 is so.

(iv) For all $a \in G$, $o(a) = o\big(f(a)\big)$.

Proof (i) Since f is a bijective function, f^{-1} exists and is also a bijective function from G_1 onto G. Now we show that f^{-1} is a homomorphism. Let $x, y \in G_1$. Then there exist $a, b \in G$ such that $f(a) = x$ and $f(b) = y$. This implies that $a = f^{-1}(x), b = f^{-1}(y)$ and $xy = f(a)f(b) = f(ab)$. Thus, $f^{-1}(xy) = ab = f^{-1}(x)f^{-1}(y)$ and so f^{-1} is a homomorphism. Hence, f^{-1} is an isomorphism.

(ii) Since f and f^{-1} are both bijective homomorphisms, we find that G_1 is a homomorphic image of G and G is a homomorphic image of G_1. Hence (ii) follows from Theorem 6.1.13(i).

(iii) Since f^{-1} is also an isomorphism, this follows from Theorem 6.1.13(ii).

(iv) By Theorem 6.1.7(iii), $o\big(f(a)\big)$ divides $o(a)$. Again since f^{-1} is a homomorphism and $f^{-1}\big(f(a)\big) = a$, we have $o(a)$ divides $o\big(f(a)\big)$. Hence $o(a) = o\big(f(a)\big)$. □

From Theorem 6.1.16(i) above, we find that if G_1 is isomorphic to G then G is also isomorphic to G_1. Henceforth, such groups will be called *isomorphic* to each other. Following are the consequences of the above theorem:

I. A finite group can never be isomorphic with an infinite group as there cannot exist a bijective function between two such groups.

II. Two groups G and G_1 may be of the same order, yet they may not be isomorphic. For example, consider the groups S_3 and Z_6; they are both finite groups

of order 6. Note that S_3 is a noncommutative group and Z_6 is a commutative group. Hence by Theorem 6.1.16(ii), we conclude that these two groups are nonisomorphic.

III. There may be two groups G and G_1 such that both of them are commutative and finite, say, $|G| = |G_1| = n$, yet they may not be isomorphic. For example, Z_4 and K_4 are both commutative groups of order 4. Z_4 is a cyclic group and K_4 is a noncyclic group, hence Z_4 and K_4 are nonisomorphic.

IV. Two groups G and G_1 may be infinite commutative groups, yet they may not be isomorphic to each other. For example, the groups $(\mathbf{Z}, +)$ and $(\mathbf{Q}, +)$ are both infinite commutative groups, yet they are nonisomorphic since $(\mathbf{Z}, +)$ is cyclic, whereas $(\mathbf{Q}, +)$ is noncyclic.

V. Two groups G and G_1 may be infinite noncyclic but commutative, yet they may not be isomorphic. For example, $(\mathbf{R}^*, \cdot)$ and $(\mathbf{C}^*, \cdot)$ are both infinite commutative groups which are not cyclic, yet they are not isomorphic because $\mathbf{C}^*$ has an element i of order 4 and $\mathbf{R}^*$ has no element of order 4. Hence by Theorem 6.1.16(iv), $\mathbf{R}^*$ and $\mathbf{C}^*$ are not isomorphic.

Regarding isomorphism of groups, we can easily prove the following properties:

I. If G is a group, then $G \simeq G$.

II. If G_1 and G_2 are any two groups such that $G_1 \simeq G_2$, then $G_2 \simeq G_1$.

III. If G_1, G_2, G_3 are any three groups such that $G_1 \simeq G_2$ and $G_2 \simeq G_3$, then $G_1 \simeq G_3$.

Hence given a group G, by an *isomorphic class of* G, we mean the collection of those groups which are isomorphic to G. So, if two groups belong to the same isomorphic class, we say that these two groups are *same upto isomorphism*. Loosely speaking, in group theory, two groups are said to be equal, if they are isomorphic groups.

We would like to draw the attention of the reader towards another very interesting feature. Observe that, on the same set G, one may define two different operations say, $*_1$ and $*_2$, in such a way that $(G, *_1)$ and $(G, *_2)$ may become two different groups. But if they are isomorphic, then we say that upto isomorphism they are equal. For example, consider the groups $(\mathbf{Z}, *_1)$ and $(\mathbf{Z}, *_2)$ on the set of all integers, where $a *_1 b = a + b$ and $a *_2 b = a + b + 1$. These are two different operations on the set $\mathbf{Z}$. For the first group, 0 is the identity element but for the second group -1 plays the role of the identity. One may easily show that the function $f : \mathbf{Z} \to \mathbf{Z}$ defined by $f(n) = n - 1$ is an isomorphism from the group $(\mathbf{Z}, *_1)$

onto the group $(\mathbb{Z}, *_2)$. Hence upto isomorphism, these two groups are regarded as same.

One important problem in the theory of groups is the *classification of groups*, where classification means the *description of isomorphic classes of groups*. In this section, we will classify all infinite cyclic groups.

Theorem 6.1.17. *Any infinite cyclic group is isomorphic to the additive group $\mathbb{Z}$ of all integers.*

Proof. Let $G = \langle a \rangle$ be an infinite cyclic group. Then $o(a)$ is not finite and this implies that $a^n = e$ if and only if $n = 0$. Define $f : \mathbb{Z} \to G$ by $f(n) = a^n$ for all $n \in \mathbb{Z}$. Clearly, f is a surjective function and $f(n+m) = a^{n+m} = a^n a^m = f(n)f(m)$ for all $n, m \in \mathbb{Z}$. Now $Ker\, f = \{n \in Z \mid f(n) = e\} = \{n \in \mathbb{Z} \mid a^n = e\} = \{0\}$. This implies that f is injective. Hence f is a bijective homomorphism and so f is an isomorphism. Consequently, $\mathbb{Z} \simeq G$.

□

From the above theorem, it follows that all infinite cyclic groups belong to the same isomorphic class of the group $(\mathbb{Z}, +)$. Hence we can say that, *upto isomorphism there exists one and only one infinite cyclic group*, which is $(\mathbb{Z}, +)$.

We conclude this section by proving the following theorem due to Cayley:

Theorem 6.1.18. [Cayley] *Every group is isomorphic to some subgroup of the group $A(S)$ of all permutations of some set S.*

Proof. Let G be a group. We take $S = G$ and consider the group $A(G)$ of all permutations on the set G. Let $a \in G$. Define $\tau_a : G \to G$ by $\tau_a(g) = ag$ for all $g \in G$. It is easy to verify that τ_a is a bijective function and hence $\tau_a \in A(G)$. Indeed, for $g_1, g_2 \in G$, $\tau_a(g_1) = \tau_a(g_2)$ implies $ag_1 = ag_2$, whence by cancellation law $g_1 = g_2$. Again, for any $g \in G$ $\tau_a(a^{-1}g) = aa^{-1}g = g$. Now for any two elements a, b of G and for any $x \in G$,

$$(\tau_a \tau_b)(x) = \tau_a\Big((\tau_b)(x)\Big) = \tau_a(bx) = a(bx) = (ab)x = \tau_{ab}(x)$$

implies that $\tau_a \tau_b = \tau_{ab}$.

Now define $\psi : G \to A(G)$ by $\psi(a) = \tau_a$ for all $a \in G$. Since for any two elements $a, b \in G$, $\tau_a \tau_b = \tau_{ab}$, hence ψ is a homomorphism.

Exercise

1. Show that $(\mathbf{C}, +) \simeq (\mathbf{R}, +) \times (\mathbf{R}, +)$.
2. For any two groups H and K, prove that $H \times K \simeq K \times H$.
3. Show that the Klein's 4-group K_4 is isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_2$.
4. Prove that for any two groups H and K, $Z(H \times K) = Z(H) \times Z(K)$.
5. Show that the group $(\mathbf{Z}, +)$ cannot be expressed as an internal direct product of two nontrivial subgroups.
6. Prove that $\mathbf{Z}_m \times \mathbf{Z}_n \simeq \mathbf{Z}_{mn}$ if and only if $gcd(m, n) = 1$.
7. Let M and N be two normal subgroups of a group G. Show that there exists a monomorphism from the group $G/M \cap N$ into the group $G/M \times G/N$.
8. Let K_i be normal subgroups of G_i, $i = 1, 2$. Show that $K_1 \times K_2$ is a normal subgroup of $G_1 \times G_2$ and $(G_1 \times G_2)/(K_1 \times K_2) \simeq G_1/K_1 \times G_2/K_2$.
9. If G_1, G_2, H_1, H_2 be groups such that $G_1 \simeq H_1$ and $G_2 \simeq H_2$, then prove that $G_1 \times G_2 \simeq H_1 \times H_2$.
10. Let H and K be two finite groups. Prove that $o(a, b) = lcm\{o(a), o(b)\}$, where $(a, b) \in H \times K$.
11. Find the number of elements of order 5 in $\mathbf{Z}_{25} \times \mathbf{Z}_5$.
12. Find all subgroups of order 7 of the group $\mathbf{Z}_7 \times \mathbf{Z}_{14}$.
13. Show that the mapping $f : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$, defined by $f\big((a, b)\big) = a - b$ is a homomorphism. Find $ker\, f$.
14. Let G be a cyclic group of order mn where $gcd(m, n) = 1$. Show that there exist subgroups H and K of order m and n respectively, such that $G \simeq H \times K$.
15. Let $\mathbf{C}^*$ be the multiplicative group of nonzero complex numbers. If $\mathbf{R}^+$ is the set of positive real numbers and $T = \{z \in \mathbf{C}^* \mid |z| = 1\}$. Then show that $\mathbf{C}^*$ is the internal direct product of $\mathbf{R}^+$ and T
16. Justify whether the following statements are true or false:
    (a) $\mathbf{Z} \times \mathbf{Z} \simeq \mathbf{Z}$.
    (b) $\mathbf{R}^* \times \mathbf{R}^* \simeq \mathbf{R}^*$.
    (c) There exists a noncyclic commutative group of order 28.
    (d) There exists a noncommutative group of order 24.
    (e) There exists a noncommutative group of order 30.
    (f) $\mathbf{Z}_6 \times \mathbf{Z}_4 \simeq \mathbf{Z}_{24}$.
    (g) $\mathbf{Z}_7 \times \mathbf{Z}_9 \simeq \mathbf{Z}_{63}$.

Find the correct answer to the following:

17. The number of subgroups of order 2 in the group $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$ is
    (i) 8 (ii) 7 (iii) 4 (iv) 1
18. The order of any nonidentity element of $\mathbf{Z}_3 \times \mathbf{Z}_3$ is
    (i) 3 (ii) 9 (iii) 6 (iv) none of these.

◊ **Exercise 7.1.2.** Show that the direct product of $S_3 \times \mathbb{Z}$ of the groups S_3 and $\mathbb{Z}$ is an infinite noncommutative group.

Solution. Since S_3 is a noncommutative group, from the Worked Out Exercise 7.1.1, it follows that the direct product $S_3 \times \mathbb{Z}$ is a noncommutative group. Now $\mathbb{Z}$ is an infinite group. Hence $S_3 \times \mathbb{Z}$ is an infinite noncommutative group.

◊ **Exercise 7.1.3.** Show that the direct product $\mathbb{Z} \times \mathbb{Z}$ is not a cyclic group.

Solution. Suppose $\mathbb{Z} \times \mathbb{Z}$ is a cyclic group. Let (n, m) be a generator of $\mathbb{Z} \times \mathbb{Z}$. We have $(1,0), (0,1) \in \mathbb{Z} \times \mathbb{Z}$. Thus there are integers r, s such that $(1,0) = r(n,m)$ and $(0,1) = s(n,m)$. But then $rn = 1$ and $sn = 0$, together imply that $s = 0$ (as $n \neq 0$, since $rn = 1$), which is a contradiction; since $stn = 1$. So it follows that $\mathbb{Z} \times \mathbb{Z}$ is not a cyclic group.

◊ **Exercise 7.1.4.** Show that the direct product $\mathbb{Z}_6 \times \mathbb{Z}_4$ of the cyclic groups $\mathbb{Z}_6$ and $\mathbb{Z}_4$ is not a cyclic group.

Solution. The elements of $\mathbb{Z}_6 \times \mathbb{Z}_4$ are the ordered pairs (u, v) where $u \in \mathbb{Z}_6$ and $v \in \mathbb{Z}_4$. Hence $|\mathbb{Z}_6 \times \mathbb{Z}_4| = 24$. In order that $\mathbb{Z}_6 \times \mathbb{Z}_4$ may be a cyclic group, it must contain an element of order 24. Now if $(a, b) \in \mathbb{Z}_6 \times \mathbb{Z}_4$, then we must have $6a = 0$ and $4b = 0$, whence $12(a, b) = (0, 0)$. This shows that order of (a, b) will not exceed 12. Hence $\mathbb{Z}_6 \times \mathbb{Z}_4$ has no element of order 24. Consequently, $\mathbb{Z}_6 \times \mathbb{Z}_4$ is not a cyclic group.

◊ **Exercise 7.1.5.** Let H and K be two finite cyclic groups of order m and n respectively. Prove that the direct product $H \times K$ is a cyclic group if and only if $gcd(m, n) = 1$.

Solution. Suppose $H \times K$ is a cyclic group and let $gcd(m, n) = d > 1$. Let $(a, b) \in H \times K$. Since $|H| = m$ and $|K| = n$, we find that $a^m = e$ and $b^n = e$. Now $\frac{m}{d}$, $\frac{n}{d}$ and $\frac{mn}{d}$ are integers and $\frac{mn}{d} < mn$.

$$(a, b)^{\frac{mn}{d}} = \left(a^{\frac{mn}{d}}, b^{\frac{mn}{d}}\right) = \left((a^m)^{\frac{n}{d}}, (b^n)^{\frac{m}{d}}\right) = (e, e).$$

This shows that the order of any element $(a, b) \in H \times K$ will be less than or equal to $\frac{mn}{d} < mn$. Hence $H \times K$, which is a group of order mn, does not contain any element of order mn. This contradicts our assumption that $H \times K$ is a cyclic group. Hence $gcd(m, n) = 1$.

Conversely, assume that $gcd(m, n) = 1$. Since H and K are both cyclic groups of order m and n respectively there exist $a \in H$ and $b \in K$ such that $o(a) = m$, $o(b) = n$. Now we show that $o(a, b) = mn$. Since $(a, b)^{mn} = (a^{mn}, b^{mn}) = \left((a^m)^n, (b^n)^m\right) = (e, e)$, the order of (a, b) is less than or equal to mn. Let d be a positive integer such that $(a, b)^d = (e, e)$. Then $a^d = e$ and $b^d = e$. Since $o(a) = m$ and $o(b) = n$, we have $m \mid d$ and $n \mid d$. Now $gcd(m, n) = 1$. Hence $mn \mid d$ and so $mn \leq d$. Thus it follows that $o(a, b) = mn$ and hence $H \times K$ is a cyclic group.

◊ **Exercise 7.1.6.** Show that the multiplicative group $\mathbb{R}^*$ of all nonzero real numbers is an internal direct product of $\mathbb{R}^+$ and T, where $\mathbb{R}^+$ is the set of all positive real numbers and $T = \{1, -1\}$

Solution. $\mathbb{R}^+$ and T are both normal subgroups of the multiplicative group $\mathbb{R}^*$. Let $a \in \mathbb{R}^*$ and $a > 0$. Then $a = a \cdot 1$ and if $a < 0$, then $a = (-a)(-1)$. Hence $\mathbb{R}^* = \mathbb{R}^+T$. Also $\mathbb{R}^+ \cap T = \{1\}$ and $ab = ba$ for all $a \in \mathbb{R}^+$ and $b \in T$. Hence $\mathbb{R}^*$ is an internal direct product of $\mathbb{R}^+$ and T.

◊ **Exercise 7.1.7.** Find the number of elements of order 5 in $\mathbb{Z}_{15} \times \mathbb{Z}_5$.

Solution. We count the number of elements (a, b) in $\mathbb{Z}_{15} \times \mathbb{Z}_5$ with the property that $5 = o(a, b) = lcm\left\{o(a), o(b)\right\}$ [cf. Problem 10 of Exercise 7.1]. If $lcm\left\{o(a), o(b)\right\} = 5$, then we have the following cases:

Case I. $o(a) = 5$, $o(b) = 5$
Case II. $o(a) = 5$, $o(b) = 1$
Case III. $o(a) = 1$, $o(b) = 5$

Case I. Since $\mathbb{Z}_{15}$ is cyclic, it contains only one subgroup of order 5 and $\mathbb{Z}_5$ is itself a subgroup of order 5 in $\mathbb{Z}_5$. In any subgroup of order 5, except identity element, every element is of order 5. Hence there are 4 choices of a and 4 choices of b. This gives 16 elements of order 5 in $\mathbb{Z}_{15} \times \mathbb{Z}_5$.

Case II. There are four choices of a and only one choice of b. This gives 4 elements of order 5 in $\mathbb{Z}_{15} \times \mathbb{Z}_5$.

Case III. There is only one choice of a and four choices of b. This gives 4 elements of order 5 in $\mathbb{Z}_{15} \times \mathbb{Z}_5$.

Thus we find that $\mathbb{Z}_{15} \times \mathbb{Z}_5$ contains 24 elements of order 5.

Proof. (i) Suppose that G is an internal direct product of the normal subgroups H and K. Then $G = HK$ and $H \cap K = \{e\}$. Hence for every $g \in G$, there are unique (prove it!) elements $a \in H$ and $b \in K$ such that $g = ab$. So we can define $f : G \to H \times K$ by $f(g) = (a, b)$ when $g = ab$, $a \in H, b \in K$. Let $g_1 = a_1b_1$ and $g_2 = a_2b_2$ be two elements of G, where $a_1, a_2 \in A$ and $b_1, b_2 \in B$. Now $g_1g_2 = a_1b_1a_2b_2 = a_1a_2b_1b_2$. Hence $f(g_1g_2) = (a_1a_2, b_1b_2) = (a_1, b_1)(a_2, b_2) = f(g_1)f(g_2)$. This shows that f is a homomorphism. Since for every $g \in G$, there are unique elements $a \in H$ and $b \in K$ such that $g = ab$, it follows that f is an injective function. Again, if $(a, b) \in H \times K$, then $g = ab \in G$ and hence $f(g) = (a, b)$. Combining all these, we find that f is an isomorphism and so $G \simeq H \times K$.

(ii) Since for each $g \in G$, there are unique elements $a \in H, b \in K$, the function $\psi : G \to H$ defined by $\psi(g) = \psi(ab) = a$, for all $g = ab \in G$ can be shown to be an epimorphism. Hence by the first isomorphism theorem $G/\ker\psi \simeq H$.

$$\begin{aligned} \text{Now, } \ker\psi &= \{g \in G \mid \psi(g) = e\} \\ &= \{g = ab \in G \mid a \in H, b \in K \text{ and } \psi(g) = e\} \\ &= \{g = ab \in G \mid a \in H, b \in K \text{ and } a = e\} \\ &= \{g = eb \in G \mid b \in K\} = K. \end{aligned}$$

Thus $G/K \simeq H$. Similarly, we can show that $G/H \simeq K$. □

Before concluding this section, we now show some applications of the concept of direct product.

Theorem 7.1.8. *Any commutative group G of order 8 is isomorphic to one of the groups $\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2$ or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, where no two of these groups are isomorphic to each other.*

Proof. Let G be a commutative group of order 8. Since $|G|$ is even, G has an element of order 2. Now G contains a finite number of elements. Hence there exists an element $a \in G$ such that $o(a) \geq o(b)$ for all $b \in G$. Clearly, $o(a) \geq 2$. Since $o(a) \mid 8$, we find that $o(a) = 8$ or 4 or 2.

Case I. Suppose $o(a) = 8$. Then G is a cyclic group of order 8 and hence $G \simeq \mathbb{Z}_8$.

Case II. Suppose $o(a) = 4$. Let $H = \langle a \rangle$. Then $|H| = 4$. Hence $H \neq G$. Let $b \in G$ such that $b \notin H$. Now H is a normal subgroup of G and hence the quotient group G/H exists and $|G/H| = 2$. Then $bH \neq H$ but $(bH)^2 = H$. Then $b^2H = H$.

This implies that $b^2 \in H = \{e, a, a^2, a^3\}$. Now $o(a) = o(a^3) = 4$. If $b^2 = a$ or a^3, then $o(b) = 8$, which goes against our assumption that $o(a) \geq o(b)$. Hence either $b^2 = e$ or $b^2 = a^2$. If $b^2 = a^2$, then $o(ba^{-1}) = 2$ and $ba^{-1} \notin H$. Thus we find that there exists an element $c \in G$ such that $c \notin H$ and $o(c) = 2$. Let $K = \langle c \rangle$. Then (i) H and K are normal subgroups (ii) $H \cap K = \{e\}$ (iii) $G = HK$. Hence $G \simeq H \times K \simeq \mathbf{Z}_4 \times \mathbf{Z}_2$.

Case III. $o(a) = 2$. Then $o(x) = 2$ for all nonidentity elements $x \in G$. Let $a, b \in G \setminus \{e\}$. Then $A = \{e, a\}, B = \{e, b\}$ are normal subgroups of G. Now $AB = \{e, a, b, ab\}$ is a subgroup of G and $AB \simeq \mathbf{Z}_2 \times \mathbf{Z}_2$. Since $AB \neq G$, there exists $c \in G$ such that $c \notin AB$. Now $o(c) = 2$. Let $C = \langle c \rangle$. Clearly, $AB \cap C = \{e\}$ abd $G = ABC$. Hence,

$$G \simeq (AB) \times C \simeq \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2.$$

Hence (upto isomorphism) there exist only three commutative groups of order 8. □

We have seen that any commutative group of order 4 is either $\mathbf{Z}_4$ or $\mathbf{Z}_2 \times \mathbf{Z}_2$; any commutative group of order 6 is $\mathbf{Z}_3 \times \mathbf{Z}_2 \simeq \mathbf{Z}_6$ and now we find that any commutative group of order 8 is either $\mathbf{Z}_8$ or $\mathbf{Z}_4 \times \mathbf{Z}_2$ or else $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$. These examples lead us towards a growing conviction that *any finite commutative group is either a cyclic group or a direct product of cyclic groups.* Indeed this is true and this result is known as the *Fundamental Theorem of finite abelian groups.*

Worked Out Exercises

◊ **Exercise 7.1.1.** Let G_1, G_2 be two groups. The direct product $G_1 \times G_2$ is commutative if and only if both G_1 and G_2 are commutative.

Solution. Suppose G_1 and G_2 are two commutative groups. Let (a_1, b_1) and (a_2, b_2) be two elements of the direct product $G_1 \times G_2$. Then $(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2) = (a_2 a_1, b_2 b_1) = (a_2, b_2)(a_1, b_1)$. Hence $G_1 \times G_2$ is a commutative group.

Conversely, assume that $G_1 \times G_2$ is a commutative group. Let $a_1, a_2 \in G_1$ and $b_1, b_2 \in G_2$. Now $(a_1, b_1), (a_2, b_2) \in G_1 \times G_2$ and so $(a_1, b_1)(a_2, b_2) = (a_2, b_2)(a_1, b_1)$, i.e., $(a_1 a_2, b_1 b_2) = (a_2 a_1, b_2 b_1)$. So we find that $a_1 a_2 = a_2 a_1$ and $b_1 b_2 = b_2 b_1$. Hence G_1 and G_2 are both commutative groups.

Proof. Clearly, the operation defined in (7.1.1) is a well-defined binary operation on $G_1 \times G_2$. The associativity of this operation follows from the group operations of G_1 and G_2. Note that (e_1, e_2) is the identity element of $G_1 \times G_2$, where e_i is the identity element of G_i, $i = 1, 2$. Finally, (a_1^{-1}, b_1^{-1}) is the inverse of (a_1, b_1) for all $(a_1, b_1) \in G_1 \times G_2$. Hence $(G_1 \times G_2, *)$ is a group.

(i) Since $(e_1, e_2) \in H_1$, $H_1 \neq \phi$. Let $(a_1, e_2), (a_2, e_2) \in H_1$. Then $(a_1, e_2)^{-1}(a_2, e_2) = (a_1^{-1}a_2, e_2^{-1}e_2) = (a_1^{-1}a_2, e_2) \in H_1$, since $a_1^{-1}a_2 \in G_1$. Now, for any $(a_1, b_1) \in G_1 \times G_2$ and $(g_1, e_2) \in H_1$, we find that $(a_1, b_1) * (g_1, e_2) * (a_1, b_1)^{-1} = (a_1 g_1 a_1^{-1}, b_1 e_2 b_1^{-1}) = (a_1 g_1 a_1^{-1}, e_2) \in H_1$. Hence H_1 is a normal subgroup. Now the function $f_1 : G_1 \to H_1$, defined by $f_1(a_1) = (a_1, e_2)$ is a bijective function and for any $a_1, a_2 \in G_1$, $f_1(a_1 a_2) = (a_1 a_2, e_2) = (a_1, e_2) * (a_2, e_2) = f_1(a_1) f_1(a_2)$. Hence $G_1 \simeq H_1$.

(ii) The proof is similar to (i).

(iii) This is a simple exercise and is left to the reader. □

Definition 7.1.2. The group $(G_1 \times G_2, *)$ of Theorem 7.1.1 is called the *external direct product* or simply *direct product* of the groups G_1 and G_2.

Henceforth, the statement "*the direct product* $G_1 \times G_2$ *of the groups* G_1 *and* G_2" will mean the group $(G_1 \times G_2, *)$. Although we have defined the direct product for a pair of groups G_1 and G_2, it is easy to see that we can extend the definition for any finite number of groups $G_1, G_2, \ldots, G_n$.

We now introduce another kind of product known as *internal direct product*.

Definition 7.1.3. Let H and K be two subgroups of a group G. G is said to be an *internal direct product* of H and K if

(a) $G = HK$,

(b) $H \cap K = \{e\}$ and

(c) $hk = kh$ for all $h \in H$ and $k \in K$.

Example 7.1.4. Consider the Klein's 4-group $K_4 = \{e, a, b, ab = ba\}$. For this group, $H_1 = \{e, a\}$ and $H_2 = \{e, b\}$ are two subgroups such that $H_1 H_2 = \{e, a\}\{e, b\} = \{e, a, b, ab\} = K_4$, $H_1 \cap H_2 = \{e\}$ and $xy = yx$ for all $x \in H_1$ and $y \in H_2$. Hence G is an internal direct product of its subgroups H_1 and H_2.

Example 7.1.5. Consider the symmetric group

$$S_3 = \{e, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}.$$

For this group, $H_1 = \{e, (1\,2)\}$ and $H_2 = \{e, (1\,2\,3), (1\,3\,2)\}$ are two subgroups such that

$$H_1H_2 = \{e, (1\,2\,3), (1\,3\,2), (1\,2), (1\,2)(1\,2\,3), (1\,2)(1\,3\,2)\}$$
$$= \{e, (1\,2\,3), (1\,3\,2), (1\,2), (2\,3), (1\,3)\} = S_3$$

and $H_1 \cap H_2 = \{e\}$. But $(1\,2)(1\,3\,2) = (1\,3) \neq (2\,3) = (1\,3\,2)(1\,2)$. Hence S_3 is not an internal direct product of the subgroups, H_1 and H_2.

Note that any group G is always an internal direct product of the trivial subgroups $\{e\}$ and G itself.

Theorem 7.1.6. *Let H and K be two subgroups of a group G. G is an internal direct product of H and K if and only if*

(i) $G = HK$

(ii) H *and* K *are normal subgroups of* G.

(iii) $H \cap K = \{e\}$.

Proof. Suppose that G is an internal direct product of the subgroups H and K. We show only that H and K are normal subgroups of G. Let $g \in G$ and $h \in H$. Since $G = HK$, there exist $h_1 \in H$ and $k_1 \in K$ such that $g = h_1k_1$. Now $ghg^{-1} = h_1k_1h(h_1k_1)^{-1} = h_1k_1hk_1^{-1}h_1^{-1} = h_1hh_1^{-1}k_1k_1^{-1}$ (since $hk = kh$ for all $h \in H, k \in K$) $= h_1hh_1^{-1} \in H$.

Hence H is a normal subgroup of G. Similarly, we can show that K is a normal subgroup of G.

Conversely, assume that all the conditions (i), (ii) and (iii) hold in G. To prove that G is an internal direct product, we have to prove only that $ab = ba$ for all $a \in H$ and $b \in K$. Consider $aba^{-1}b^{-1}$. Now $aba^{-1}b^{-1} \in a(bHb^{-1}) \subseteq aH = H$ (since $a \in H$) and $aba^{-1}b^{-1} \in (aKa^{-1})b^{-1} \subseteq Kb^{-1} = K$ (since $b^{-1} \in K$). Hence $aba^{-1}b^{-1} \in H \cap K = \{e\}$ and so $ab = ba$ for all $a \in H, b \in K$. This completes the proof. □

Theorem 7.1.7. *Let G be a group and H, K be two normal subgroups of G. If G is an internal direct product of H and K then,*

(i) $G \simeq H \times K$,

(ii) $G/H \simeq K$ *and* $G/K \simeq H$.

Chapter 7

Direct Product of Groups

In this section, we shall show that given n groups $G_1, G_2, \ldots, G_n$, we can construct a new group G, such that each G_i can be considered as a subgroup of this group.

7.1 Direct Product

Let G_1 and G_2 be two groups. Now, the Cartesian product of the sets G_1 and G_2 is the set $G_1 \times G_2$ of all ordered pairs (a_1, b_1), where $a_1 \in G_1$ and $b_1 \in G_2$. Define a binary operation $*$ on $G_1 \times G_2$ as follows:

$$(a_1, b_1) * (a_2, b_2) = (a_1 a_2, b_1 b_2) \text{ for all } (a_1, b_1), (a_2, b_2) \in G_1 \times G_2 \qquad (7.1.1)$$

Here $a_1 a_2$ denotes that product of a_1 and a_2 in the group G_1 and $b_1 b_2$ denotes the product of b_1 and b_2 in the group G_2.

Let us show that $G_1 \times G_2$ is a group under this binary operation, such that G_1 is isomorphic to a subgroup of this group and so is G_2.

Theorem 7.1.1. *Let G_1 and G_2 be two groups. Then the set*

$$G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1 \text{ and } g_2 \in G_2\}$$

is a group under the binary operation defined in (7.1.1). Furthermore,

(i) $H_1 = \{(a_1, e_2) \in G_1 \times G_2 \mid e_2$ *is the identity element of* $G_2\}$ *is a normal subgroup of* $G_1 \times G_2$ *and* $G_1 \simeq H_1$.

(ii) $H_2 = \{(e_1, b_2) \in G_1 \times G_2 \mid e_1$ *is the identity of* $G_1\}$ *is a normal subgroup of* $G_1 \times G_2$ *such that* $G_2 \simeq H_2$.

(iii) $G_1 \times G_2 = H_1 H_2 = H_2 H_1, \quad H_1 \cap H_2 = \{(e_1, e_2)\}$.

$$\begin{aligned} \ker f &= \{g \in G \mid f(g) = \text{identity of } G/H\} \\ &= \{g \in G \mid f(g) = eH\} \\ &= \{g \in G \mid gH = eH = H\} \\ &= \{g \in G \mid g \in H\} \\ &= H. \end{aligned}$$

Exercise

1. Let T be the group of all complex numbers z such that $|z| = 1$. Show that $C^*/T \simeq \mathbb{R}^+$
2. Prove that $7\mathbb{Z}/56\mathbb{Z} \simeq \mathbb{Z}_8$.
3. Prove that $6\mathbb{Z}/30\mathbb{Z}$ is isomorphic to $\mathbb{Z}_5$.
4. If G is an infinite group such that G is a homomorphic image of $\mathbb{Z}$, then prove that $G \simeq \mathbb{Z}$.
5. Show that $\mathbb{Z}_{16}$ is not a homomorphic image of $\mathbb{Z}_4 \times \mathbb{Z}_4$
6. Let T be the group of all complex numbers ω, such that $|\omega| = 1$. (This group is called *circle group*). Show that $\mathbb{R}/\mathbb{Z} \simeq T$, where $\mathbb{R}$ is the additive group of all real numbers
7. Let H be a normal subgroup of order 6. If $f : G \to G_1$ be an epimorphism of groups such that $H \subseteq \ker f$, then show that G_1 is also a homomorphic image of G/H.
8. Find all subgroups of the groups $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/24\mathbb{Z}$.
9. Show that if there exists an epimorphism from a finite group G onto the group $\mathbb{Z}_{35}$, then G has normal subgroups of index 7 and 5.
10. If there exists an epimorphism from a finite group G onto the group $\mathbb{Z}_8$, then show that G has normal subgroups of index 4 and 2.
11. Which of the following statements are true? Justify.
    (a) $\mathbb{Z}_6$ has six homomorphic images.
    (b) The quotient group $5\mathbb{Z}/45\mathbb{Z}$ has three subgroups.
    (c) $4\mathbb{Z}/16\mathbb{Z}$ is a subgroup of $\mathbb{Z}/16\mathbb{Z}$.
    (d) There are 5 subgroups of $\mathbb{Z}$ which contain $20\mathbb{Z}$ as a subgroup.
    (e) Any epimorphism of $\mathbb{Z}$ onto $\mathbb{Z}$ is an isomorphism.
    (f) There exists an epimorphism $f : \mathbb{Z}_{24} \to \mathbb{Z}_5$.

Find the correct answer to the following:

12. The number of subgroups of the group $\mathbb{Z}/10\mathbb{Z}$ is
    (i) 1 (ii) 10 (iii) 4 (iv) 5.
13. The number of subgroups of the quotient group $4\mathbb{Z}/12\mathbb{Z}$ is
    (i) 3 (ii) 2 (iii) 4 (iv) 1.

Worked Out Exercises

where $GL(2,\mathbb{R})$ be the group of all non-singular 2×2 matrices over $\mathbb{R}$. and $SL(2,\mathbb{R})$ be the group of 2×2 matrices over $\mathbb{R}$ with determinant 1.

Exercise 6.2.1. Show that $GL(2,\mathbb{R})/SL(2,\mathbb{R}) \simeq \mathbb{R}^*$.

IAS-2010

Solution. Define $f : GL(2,\mathbb{R}) \to \mathbb{R}^*$ by $f(A) = \det A$ for all $A \in GL(2,\mathbb{R})$. We have shown in Example 6.1.4 that f is a homomorphism. Let $a \in \mathbb{R}^*$. Then $A = \begin{bmatrix} 1 & 0 \\ 0 & a \end{bmatrix} \in GL(2,\mathbb{R})$ and $f(A) = \det A = a$. Hence f is an epimorphism and so by the First Isomorphism theorem,

$$GL(2,\mathbb{R})/\ker f \simeq \mathbb{R}^*.$$

Now, $\ker f = \{A \in GL(2,\mathbb{R}) \mid \det A = 1\} = SL(2,\mathbb{R})$. Hence,

$$GL(2,\mathbb{R})/SL(2,\mathbb{R}) \simeq \mathbb{R}^*.$$

Exercise 6.2.2. Prove that the group $4\mathbb{Z}/12\mathbb{Z} \simeq \mathbb{Z}_3$.

Solution. Define $f : 4\mathbb{Z} \to \mathbb{Z}_3$ by $f(4n) = [n]$ for all $n \in \mathbb{Z}$. Clearly, f is surjective and

$$f(4n+4m) = f\big(4(n+m)\big) = [n+m] = [n] + [m] = f(4n) + f(4m).$$

Hence f is an epimorphism. So by the First Isomorphism theorem,

$$4\mathbb{Z}/\ker f \simeq \mathbb{Z}_3.$$

Now

$$\begin{aligned} \ker f &= \{4n \in 4\mathbb{Z} \mid f(4n) = [0] \text{ in } \mathbb{Z}_3\} \\ &= \{4n \in 4\mathbb{Z} \mid [n] = [0] \text{ in } \mathbb{Z}_3\} \\ &= \{4n \in 4\mathbb{Z} \mid n \text{ is a multiple of } 3\} \\ &= \{4n \in 4\mathbb{Z} \mid n = 3k,\ k \in \mathbb{Z}\} \\ &= 12\mathbb{Z} \end{aligned}$$

Hence the result follows.

◊ **Exercise 6.2.3.** Find all homomorphic images of the additive group $\mathbb{Z}$.

Solution. The subgroups of $\mathbb{Z}$ are given by $n\mathbb{Z}, n \in \mathbb{N}_0$. Since $\mathbb{Z}$ is commutative, all these subgroups of $\mathbb{Z}$ are normal subgroups of $\mathbb{Z}$. Thus the homomorphic images of $\mathbb{Z}$ are the groups, $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$, $n = 0,1,2$.

◊ **Exercise 6.2.4.** Show that $\mathbb{Z}_9$ is not a homomorphic image of $\mathbb{Z}_{16}$.

Solution. Suppose there exists an epimorphism $f : \mathbb{Z}_{16} \to \mathbb{Z}_9$. Then by the First Isomorphism theorem, $\mathbb{Z}_{16}/\ker f \simeq \mathbb{Z}_9$. Hence $\left|\mathbb{Z}_{16}/\ker f\right| = |\mathbb{Z}_9| = 9$. This shows that

$$\frac{|\mathbb{Z}_{16}|}{|\ker f|} = 9,$$

i.e., $9 \cdot |\ker f| = 16$. This is absurd. Hence $\mathbb{Z}_9$ is not a homomorphic image of $\mathbb{Z}_{16}$.

◊ **Exercise 6.2.5.** Find all the subgroups of $\mathbb{Z}/21\mathbb{Z}$.

Solution. Let K be a subgroup of $\mathbb{Z}/21\mathbb{Z}$. Then $K = H/21\mathbb{Z}$ for some subgroup H of $\mathbb{Z}$ such that $21\mathbb{Z} \subseteq H$. Again, if H is a subgroup of $\mathbb{Z}$, such that $21\mathbb{Z} \subseteq H$, then $H/21\mathbb{Z}$ is a subgroup of $\mathbb{Z}/21\mathbb{Z}$. So we have to determine all subgroups of $\mathbb{Z}$ that contain $21\mathbb{Z}$. Now, 1, 3, 7, 21 are the only positive divisors of 21. Hence $\mathbb{Z}$, $3\mathbb{Z}$, $7\mathbb{Z}$ and $21\mathbb{Z}$ are the only subgroups of $\mathbb{Z}$ that contain $21\mathbb{Z}$. Then $\mathbb{Z}/21\mathbb{Z}$, $3\mathbb{Z}/21\mathbb{Z}$, $7\mathbb{Z}/21\mathbb{Z}$ and $21\mathbb{Z}/21\mathbb{Z}$ are the only subgroups of $\mathbb{Z}/21\mathbb{Z}$.

◊ **Exercise 6.2.6.** If there exists an epimorphism from a finite group G onto the group $\mathbb{Z}_{15}$, then show that G has normal subgroups of indices 5 and 3.

Solution. Let $f : G \to \mathbb{Z}_{15}$ be an epimorphism of groups. Then by the First Isomorphism theorem, $G/\ker f \simeq \mathbb{Z}_{15}$. Hence $G/\ker f$ is a cyclic group of order 15. Now 5 divides 15. Hence $G/\ker f$ has a subgroup K of order 5. Since $G/\ker f$ is commutative, K is a normal subgroup. Then $K = H/\ker f$ for some normal subgroup H of G such that $\ker f \subseteq H \subseteq G$. Now,

$$15 = |\mathbb{Z}_{15}| = \left|G/\ker f\right| = \frac{|G|}{|H|} \cdot \frac{|H|}{|\ker f|} = [G : H] \cdot \left|H/\ker f\right| = [G : H] \cdot 5.$$

This shows that $[G : H] = 3$. Since 3 also divides 15, proceeding as above, we can show that G has a normal subgroup of index 5.

◊ **Exercise 6.2.7.** Let G be a group and H be a normal subgroup of G. Then show that there exists an epimorphism $f : G \to G/H$ such that $\ker f = H$.

Solution. Define the mapping $f : G \to G/H$ by $f(g) = gH$. Clearly, the mapping is well-defined. Let $g_1, g_2 \in G$. Then $f(g_1g_2) = g_1g_2H = g_1H \cdot g_2H = f(g_1)f(g_2)$, whence it follows that f is a homomorphism. Let $x \in G/H$. Then $x = gH$ for some $g \in G$. This implies $x = gH = f(g)$ and hence f is onto, i.e., f is an epimorphism of G onto G/H. Now,

$$\begin{aligned} \text{Now,} \quad \ker f &= \{h \in H \mid f(h) = \text{identity element of } HK/K\} \\ &= \{h \in H \mid hK = K\} \\ &= \{h \in H \mid h \in K\} \\ &= H \cap K. \end{aligned}$$

Consequently, $H/H \cap K \simeq (HK)/K$. □

Theorem 6.2.10. [Third Isomorphism Theorem] : *Let H_1 and H_2 be two normal subgroups of a group G such that $H_1 \subseteq H_2$. Then,*

$$(G/H_1)/(H_2/H_1) \simeq G/H_2.$$

Proof. Define $f : G/H_1 \to G/H_2$ by $f(aH_1) = aH_2$ for all $a \in G$. We leave it for the reader to verify that f is well-defined. Clearly, f is an epimorphism. By the First Isomorphism theorem,

$$(G/H_1)/\ker f \simeq G/H_2.$$

Now,

$$\begin{aligned} \ker f &= \{aH_1 \in G/H_1 \mid f(aH_1) = eH_2\} \\ &= \{aH_1 \in G/H_1 \mid aH_2 = eH_2\} \\ &= \{aH_1 \in G/H_1 \mid a \in H_2\} \\ &= H_2/H_1. \end{aligned}$$

This completes the proof. □

We have seen that for any normal subgroup K of a group G, the quotient group G/K is a homomorphic image of G. Now what are the subgroups and normal subgroups of G/K?

Theorem 6.2.11. *Let K be a normal subgroup of a group G.*

(i) If H is a subgroup of G such that $K \subseteq H$, then $H/K = \{aK \mid a \in H\}$ is a subgroup of G/K.

(ii) If T is a subgroup of G/K, then there exists a subgroup H of G such that $K \subseteq H$ and $T = H/K$.

(iii) The function ψ defined by $\psi(H) = H/K$ from the set of all subgroups of G that contain K and the set $\mathcal{B}$ of all subgroups of G/H. is a bijective function.

(iv) The function ψ as described in (iii) preserves inclusion relation, i.e., $K \subseteq H_1 \subseteq H$ if and only if $H_1/K \subseteq H/K$.

(v) H is a normal subgroup of G with $K \subseteq H$, if and only if H/K is a normal subgroup of G/K.

Proof. (i) The function $f : G \to G/K$ defined by $f(a) = aK$ is an epimorphism. Now by Theorem 6.1.7(i), $f(H) = \{aK \mid a \in H\}$ is a subgroup of G/K. Hence H/K is a subgroup of G/K.

(ii) Let T be a subgroup of G/K. Then by the Theorem 6.1.7(ii), $f^{-1}(T)$ is a subgroup of G. Now $f^{-1}(T) = \{a \in G \mid f(a) \in T\} = \{a \in G \mid aK \in T\}$. Let $H = \{a \in G \mid aK \in T\}$. Suppose $u \in K$, Then, $uK = K$ is the identity element of G/K and so $uK \in T$. Hence $u \in H$. This implies that $K \subseteq H$. Since $f(H) = \{aK \mid a \in H\} = \{aK \mid aK \in T\} = T$, it follows that $T = H/K$.

(iii) Clearly, ψ is surjective. Now suppose that H_1 and H_2 be two subgroups of G such that $K \subseteq H_1$, $K \subseteq H_2$ and $f(H_1) = f(H_2)$. Then $H_1/K = H_2/K$. Let $a \in H_1$. Then $aK = bK$ for some $b \in H_2$. Hence $b^{-1}a \in K \subseteq H_2$ and so $a = b(b^{-1}a) \in H_2$. Thus we find that $H_1 \subseteq H_2$. Similarly, we can show that $H_2 \subseteq H_1$ and then $H_1 = H_2$ which implies that ψ is injective.

(iv) If $H_1 \subseteq H$, then clearly, $H_1/K \subseteq H/K$. Conversely, assume that $H_1/K \subseteq H/K$. Let $a \in H_1$. Then $aK \in H_1/K \subseteq H/K$. Hence $aK = hK$ for some $h \in H$. Hence $h^{-1}a \in K \subseteq H$ and so, $a = h(h^{-1}a) \in H$. Thus we find that $H_1 \subseteq H$.

(v) Since the natural homomorphism $f : G \to G/K$ is an epimorphism, it follows that if H is a normal subgroup of G, then $f(H) = H/K$ is also a normal subgroup of G/H. Conversely, assume that T is a normal subgroup of G/K. Then by (ii), $T = H/K$ where H is a subgroup of G such that $K \subseteq H$. Let $g \in G$. Then $gK(H/K)(gK)^{-1} \subseteq H/K$. Let $h \in H$. We find that $gKhK(gK)^{-1} \in H/K$, i.e., $(ghg^{-1})K \in H/K$. Hence $ghg^{-1} \in H$. This proves that H is a normal subgroup of G. □

Now we can generalize this theorem and prove the following:

Theorem 6.2.12. *Let $f : G \to G_1$ be an epimorphism of groups. Let*

$$\mathcal{H} = \{H \mid H \text{ is a subgroup of } G \text{ that contains } \ker f\}$$

and

$$\mathcal{K} = \{K \mid K \text{ is a subgroup of } G_1\}.$$

Then the function $f^* : \mathcal{H} \to \mathcal{K}$ defined by $f^*(H) = f(H)$ for all $H \in \mathcal{H}$ is an inclusion preserving bijective function and $f^*(H)$ is a normal subgroup of G_1 if and only if H is a normal subgroup of G.

Proof. Since f is an epimorphism, by the First Isomorphism theorem, $G_1 \simeq G/\ker f$. So the proof is analogous to the Theorem 6.2.11 and we leave it to the reader. □

$|G| = 6$, it cannot have a subgroup of order 4. Hence, there exists $b \in G$ such that $b^2 \neq e$, i.e., $b \neq e$ and $o(b) \neq 2$. Since $o(b)$ must be a divisor of 6, we have $o(b) = 6$ or 3. If $o(b) = 6$, then $G = \langle b \rangle$ is a cyclic group of order 6 and $G \simeq \mathbb{Z}_6$. Suppose G is not cyclic. Then $o(b) = 3$. Let $H = \{e, b, b^2\}$. Then H is a subgroup of G of index 2. Thus, H is a normal subgroup of G (by Worked Out Exercise 5.4.1). Clearly $a \notin H$. Now $G = H \cup aH$ and $H \cap aH = \emptyset$. Hence, $G = \{e, b, b^2, a, ab, ab^2\}$. Now $aba^{-1} \in H$, since H is normal and $b \in H$. This tells us that aba^{-1} is any one of the elements e, b, b^2. If $aba^{-1} = e$, then $b = e$, which is a contradiction. If however, $aba^{-1} = b$, then $ab = ba$. Since $o(a)$ and $o(b)$ are relatively prime and $ab = ba$, we must have $o(ab) = o(a) \cdot o(b) = 2 \cdot 3 = 6$, whence in this case G becomes cyclic, again a contradiction. This leaves us with the option $aba^{-1} = b^2$. Thus $G = \langle a, b \rangle$, where $o(a) = 2$, $o(b) = 3$ and $ab = b^2a$. It is now easy to see that $G \simeq S_3$. □

In the aforesaid discussions, we have tacitly justified another significant fact. Can you appreciate now that the *smallest noncommutative group* is of order 6?

From the first isomorphism theorem we find that if a group G_1 is a homomorphic image of a group G, then the group G_1 is nothing but $G/\ker f$. Now if H is any normal subgroup of a group G, then the function $f : G \to G/H$, defined by $f(a) = aH$ is an epimorphism with $\ker f = H$, which is called the *natural homomorphism* or the *canonical homomorphism* of G onto G/H. Hence *all the homomorphic images of a group G are the groups G/H, where H is a normal subgroup of G*. Conversely, *every normal subgroup H of a group G is the kernel of some homomorphism*, viz., the natural homomorphism defined above. [cf. Worked Out Exercise 6.2.7].

The following diagram (Fig. 14) depicts the natural homomorphism:

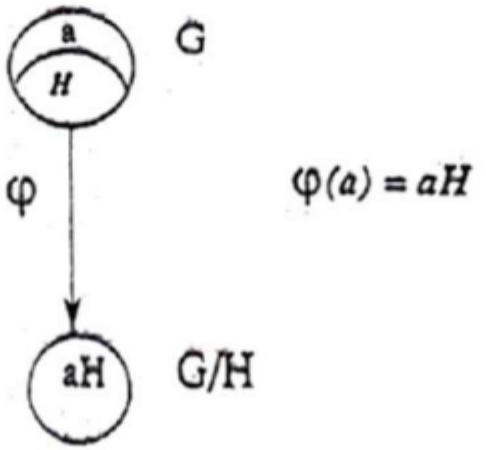


Fig. 14

In the light of the aforesaid discussions, we can now complete the diagram (Fig. 15) given with the first isomorphism theorem as below:

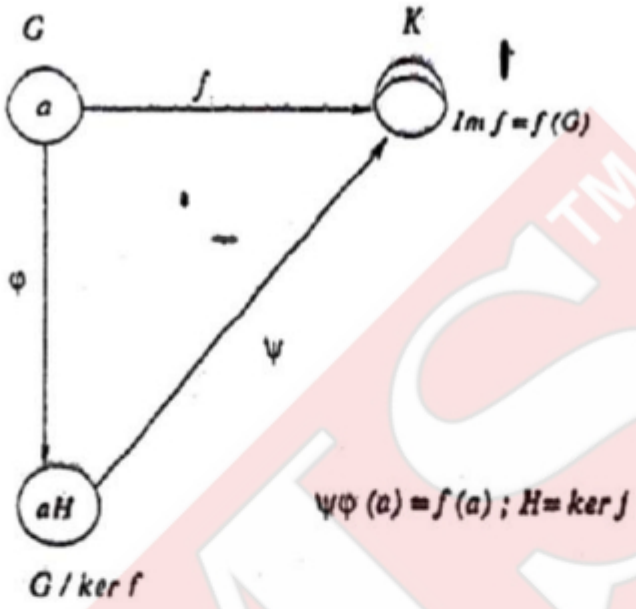


Fig. 15

Example 6.2.8. Consider the group S_3. This group has only three normal subgroups, which are S_3, A_3, and $\{e\}$. Hence all the homomorphic images of S_3 are S_3/S_3, S_3/A_3, and $S_3/\{e\}$. Now S_3/S_3 is a group with only one element, whence $S_3/S_3 \simeq \{e\}$. Again S_3/A_3 is a group of order $\frac{|S_3|}{|A_3|} = \frac{6}{3} = 2$. Hence $S_3/A_3 \simeq Z_2$. Finally $S_3/\{e\} \simeq S_3$. So we find that $\{e\}, Z_2$ and S_3 are the only homomorphic images of S_3.

Theorem 6.2.9. [Second Isomorphism Theorem] : *Let H and K be subgroups of a group G with K normal in G. Then,*

$$H/(H \cap K) \simeq (HK)/K.$$

Proof. Define $f : H \to (HK)/K$ by $f(h) = hK$ for all $h \in H$. Now $f(h_1 h_2) = h_1 h_2 K = h_1 K h_2 K = f(h_1) f(h_2)$ for all $h_1, h_2 \in H$, proving that f is a homomorphism. Let $xK \in (HK)/K$. Then $x = hk$ for some $h \in H$ and $k \in K$. Thus, $xK = (hk)K = (hK)(kK) = hK = f(h)$. This proves that f is onto and so $f(H) = (HK)/K$. Hence by the first isomorphism theorem, it follows that

$$H/\ker f \simeq (HK)/K.$$

To complete the proof, we now show that $\ker f = H \cap K$.

$f(a) = f(b)$. Consequently, $\psi(aH) = f(a) = f(b) = \psi(bH)$ and so ψ is well-defined. Now for any $xH, yH \in G/H$, $\psi(xHyH) = \psi(xyH) = f(xy) = f(x)f(y)$. Hence ψ is a homomorphism. Since $Im(f) = f(G)$, we find that, for any $a \in Im\, f$, there exists $u \in G$ such that $f(u) = a$ and then $uH \in G/H$, which shows that $\psi(uH) = f(u) = a$. So, ψ is surjective. Let $aH, bH \in G/H$, such that $\psi(aH) = \psi(bH)$. Then $f(a) = f(b)$. Hence $f(a^{-1}b) = f(a)^{-1}f(b) = f(b)^{-1}f(b) = e_1$ implies that $a^{-1}b \in ker\, f = H$. Thus it follows that $aH = bH$ and so ψ is injective. Hence ψ is an isomorphism. □

Corollary 6.2.2. *If $f : G \to G_1$ be an epimorphism of groups, then $G/Ker\, f \simeq G_1$.*

Proof. Since f is an epimorphism, f is surjective and hence $Im\, f = G_1$. Therefore from Theorem 6.2.1, $G/ker\, f \simeq G_1$. □

Corollary 6.2.3. *For any group G, $G/\{e\} \simeq G$, where $\{e\}$ is the subgroup containing the identity element e of G.*

Proof. The identity function $I_G : G \to G$, defined by $I_G(x) = x$ for all $x \in G$, is an epimorphism such that $ker\, I_G = \{e\}$. Hence $G/\{e\} \simeq G$. □

Theorem 6.2.4. *If G is a finite cyclic group of order n, $G \simeq \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$.*

Proof. Let $G = \langle a \rangle$, where a is an element of order n in G. Define $f : \mathbb{Z} \to G$ by $f(m) = a^m$, for all $m \in \mathbb{Z}$. For any two integers m and r, $f(m + r) = a^{m+r} = a^m a^r = f(m)f(r)$. Hence f is a homomorphism. Let $x \in G$. Then $x = a^t$ for some $t \in \mathbb{Z}$. Then $f(t) = a^t = x$. Hence f is an epimorphism. Then by the First Isomorphism theorem, $\mathbb{Z}/ker\, f \simeq Im\, f = G$. Here,

$$\begin{aligned} ker\, f &= \{m \in \mathbb{Z} \mid f(m) = \text{ identity element of } G\} \\ &= \{m \in \mathbb{Z} \mid a^m = e\} \\ &= \{m \in \mathbb{Z} \mid n \text{ divides } m\} \quad [\text{as } o(a) = n] \quad = n\mathbb{Z}. \end{aligned}$$

Hence $\mathbb{Z}/n\mathbb{Z} \simeq G$. Now define $g : \mathbb{Z} \to \mathbb{Z}_n$ by $g(t) = [t]$. It is easy to see that g is an epimorphism and $ker\, g = n\mathbb{Z}$. Hence $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$. So it follows that $G \simeq \mathbb{Z}_n$. □

Corollary 6.2.5. *Any two finite cyclic groups of same order are isomorphic.*

From the above theorem, it follows that, up to isomorphism there exists one and only one cyclic group of order n, for every positive integer n. Thus we have found all finite cyclic groups. These are precisely $\mathbb{Z}_1, \mathbb{Z}_2, \mathbb{Z}_3, \ldots, \mathbb{Z}_n, \ldots\ldots$

Since every group of prime order is cyclic, we find from the above that *for each prime integer p, there exists one and only one group (upto isomorphism) of order p, which is $\mathbb{Z}_p$.*

This tells us that $\mathbb{Z}_2$ and $\mathbb{Z}_3$ are the only groups of order 2 and order 3 respectively. Now what are the groups of order 4? The next theorem will throw some light.

Theorem 6.2.6. *Upto isomorphism, there are only two groups of order four.*

Proof. The groups $\mathbb{Z}_4$ and K_4 (Klein's 4-group) are groups of order 4. Observe that $\mathbb{Z}_4$ is a cyclic group, whereas K_4 is noncyclic. Hence these two groups are nonisomorphic. We assert that these two are the only groups (upto isomorphism) of order 4. Towards the proof of our assertion, we show that any group of order 4 is isomorphic to either $\mathbb{Z}_4$ or K_4. If G is a cyclic group of order 4, then by Theorem 6.2.4, $G \simeq \mathbb{Z}_4$. Suppose now that G is noncyclic. Then no element in G can be of order 4. As otherwise, if $a \in G$ be of order 4, then $\langle a \rangle = G$ shows that G is cyclic, which is a contradiction. Let $G = \{e, a, b, c\}$. Since the order of every element of G must divide the order of G, we see that the order of each of a, b, c must be 2. If $ab = a$, then $b = e$, which is not possible, whence we have $ab \neq a$. Similarly, $ab \neq b$. Suppose $ab = e$; then $a(ab) = ae$, whence $b = a$, (since $a^2 = e$) which is not possible either and this shows that we are left out with the only possibility that $ab = c$. Similarly, we may show $ba = c$. Hence $ab = ba$. Thus we find that $G = \langle a, b \rangle$ such that $o(a) = o(b) = 2$ and $ab = ba$. Hence G is the Klein's 4-group K_4. Hence the theorem. □

Continuing our pursuit of distinct finite groups, we point out that $\mathbb{Z}_5$ is the only group of order 5. The next theorem shows that there are only two nonisomorphic groups of order 6.

Theorem 6.2.7. *There are only two (upto isomorphism) groups of order six.*

Proof. Evidently, $\mathbb{Z}_6$ is a cyclic group of order 6 and hence commutative, whereas S_3 is a noncommutative group of order 6. This clearly shows that these two groups are nonisomorphic. It will now be sufficient to show that any group of order 6 is either isomorphic to $\mathbb{Z}_6$ or to S_3.

Let G be a group of order 6. Since $|G|$ is even, there exists $a \in G$, $a \neq e$ such that $a^2 = e$. If $x^2 = e$ for all $x \in G$, then G is commutative and for any two distinct nonidentity elements a and b of G, $\{e, a, b, ab\}$ must be a subgroup of G. But since

4. Find all epimorphisms from $(\mathbb{Z}, +)$ onto $(\mathbb{Z}, +)$.
5. Find all homomorphisms from $(\mathbb{Z}, +)$ onto $(\mathbb{Z}_6, +)$.
6. Find all homomorphisms from $(\mathbb{Z}_6, +)$ into $(\mathbb{Z}_4, +)$.
7. Show that $(\mathbb{Z}, +)$ and $(\mathbb{R}, +)$ are not isomorphic groups.
8. Show that $\mathbb{Q}^*$, the group of all nonzero rational numbers under multiplication, is not isomorphic to $\mathbb{R}^*$, the group of all nonzero real numbers under multiplication.
9. Show that $(\mathbb{Q}, +)$ and $(\mathbb{Q}, \cdot)$ are not isomorphic groups.
10. Show that $(\mathbb{Q}, +)$ and $(\mathbb{R}, +)$ are not isomorphic groups.
11. Show that there exists an isomorphism from the group $(\mathbb{C}, +)$ onto the group $\mathbb{R} \times \mathbb{R}$.
12. Let G be a group. Prove that the function $f : G \to G$ defined by $f(a) = a^{-1}$ for all $a \in G$ is a homomorphism if and only if G is commutative.
13. Show that S_3 and $\mathbb{Z}_6$ are nonisomorphic groups and for every proper subgroup A of S_3 there exists a proper subgroup B of $\mathbb{Z}_6$ such that $A \simeq B$.
14. Let G, H and K be groups. Suppose that the functions $f : G \to H$ and $g : H \to K$ are homomorphisms. Prove that $g \circ f : G \to K$ is also a homomorphism.
15. Let G, H and K be three groups. If $G \simeq H$ and $H \simeq K$, then prove that $G \simeq K$.
16. Let G and H be groups. Define a function $f : G \times H \to G$ by $f((a, b)) = a$ for all $(a, b) \in G \times H$. Prove that f is a homomorphism from $G \times H$ onto G. Determine $\ker f$.
17. Show that every commutative group of order 6 is a cyclic group.
18. Which of the following statements are true? Justify.

    (a) A noncommutative group may be a homomorphic image of a commutative group.

    (b) A cyclic group with more than one element may be a homomorphic image of a noncyclic group.

    (c) There does not exist a nontrivial homomorphism from a group G of order 5 into a group H of order 4.

    (d) The group $(2\mathbb{Z}, +)$ is isomorphic to the group $(3\mathbb{Z}, +)$.

    (e) The group $(\mathbb{Z}, +)$ is isomorphic to $(\mathbb{Q}, +)$.

    (f) There exists a monomorphism from a group of order 30 into a group of order 100.

    (g) There exists an epimorphism from $(\mathbb{Z}, +)$ onto $(\mathbb{R}, +)$.

    (h) There does not exist any epimorphism of $(\mathbb{Q}, +)$ onto $(\mathbb{Z}, +)$.

    (i) If f and g are two epimorphisms of a group G onto a group H such that $\ker f = \ker g$, then $f = g$.

    (j) There exists a permutation group of order n, for each $n \in \mathbb{N}$.

Find the correct answer to the following.

19. The number of isomorphisms from the group $\mathbb{Z}$ onto the group $\mathbb{Z}$ is
(i) 0 (ii) 1 (iii) 2 (iv) infinite.

20. The number of homomorphisms from the group $(\mathbb{Z}_8, +)$ onto the group $(\mathbb{Z}_4, +)$ is
(i) 6 (ii) 4 (iii) 1 (iv) 2.

Isomorphism Theorems

In this section, we shall prove some of the most classical theorems of group theory that have a trend-setting character for the line of investigation of almost all branches in abstract algebra. These theorems, in the context of group theory, reveal the interplay between homomorphisms and quotient groups.

Theorem 6.2.1. [First Isomorphism Theorem] : *Let $f : G \to G_1$ be a homomorphism of groups. Then the quotient group $G/\ker f$ is isomorphic to the subgroup $Im\, f$ of G_1.*

Proof. The following diagram (Fig. 13) may be of help in appreciating the proof.

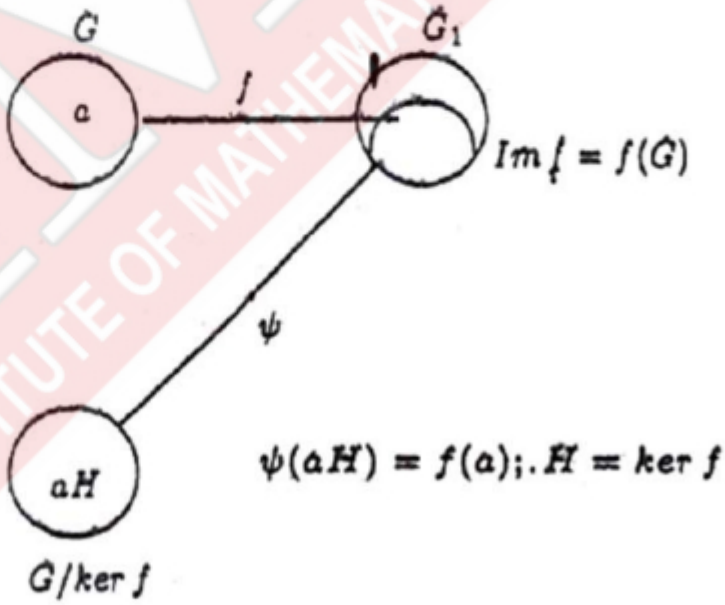


Fig. 13

Let $H = \ker f$. We show that $G/H \simeq Im\, f$: Define a function $\psi : G/H \to Im\, f$ by $\psi(aH) = f(a)$, for all $aH \in G/H$. We first show that ψ is well-defined. For this, let $aH = bH$ in G/H. Then $a^{-1}b \in H = \ker f$ and so $f(a^{-1}b) = e_1$, where e_1 is the identity of G_1. This implies that $e_1 = f(a^{-1})f(b) = f(a)^{-1}f(b)$ and hence

$$\begin{aligned} \ker f &= \{\sigma \in S_3 \mid f(\sigma) = 1\} \\ &= \{\sigma \in S_3 \mid \sigma \text{ is even}\} \\ &= A_3. \end{aligned}$$

◊ **Exercise 6.1.3.** Show that the group $(\mathbb{Z}_6, +)$ is a homomorphic image of the group $(\mathbb{Z}, +)$.

Solution. Define $f : \mathbb{Z} \to \mathbb{Z}_6$ by $f(n) = [n]$ for all $n \in \mathbb{Z}$. Let $n, m \in \mathbb{Z}$. Then $f(n + m) = [n + m] = [n] + [m] = f(n) + f(m)$. Hence f is a homomorphism. Let $[r] \in \mathbb{Z}_6$. Then $r \in \mathbb{Z}$ and hence $f(r) = [r]$. This shows that f is surjective and so f is an epimorphism. Consequently, $\mathbb{Z}_6$ is a homomorphic image of $\mathbb{Z}$.

◊ **Exercise 6.1.4.** Let $f : G \to G_1$ be an epimorphism of groups. If H is a normal subgroup of G, then show that $f(H)$ is a normal subgroup of G_1.

Solution. By Theorem 6.1.7(1), we know that $f(H)$ is a subgroup of G_1. Let $g_1 \in G_1$. Since $f(G) = G_1$, there exists $g \in G$ such that $f(g) = g_1$. Now for any $h \in H$, $g_1 f(h) g_1^{-1} = f(g) f(h) f(g)^{-1} = f(ghg^{-1})$. Since H is a normal subgroup of G, $ghg^{-1} \in H$, and so $g_1 f(h) g_1^{-1} \in f(H)$. Thus $g_1 f(H) g_1^{-1} \subseteq f(H)$. Hence $f(H)$ is a normal subgroup of G_1.

◊ **Exercise 6.1.5.** Find all the homomorphisms of the group $(\mathbb{Z}, +)$ to the group $(\mathbb{Z}, +)$.

Solution. Let n be an integer. Define $f : \mathbb{Z} \to \mathbb{Z}$ by $f(t) = nt$ for all $t \in \mathbb{Z}$. Let $r, s \in \mathbb{Z}$. Then $f(r + s) = n(r + s) = nr + ns = f(r) + f(s)$. Hence f is a homomorphism. We denote this homomorphism by f_n. We show that any homomorphism from $\mathbb{Z}$ to $\mathbb{Z}$ is one of these $f_n, n \in \mathbb{Z}$. To show this, let us consider an integer $m \in \mathbb{Z}$. Now if f is a homomorphism from $\mathbb{Z}$ to $\mathbb{Z}$, then $f(m) = f(m1) = mf(1)$ (by Theorem 6.1.6(iii)) $= f(1)m$. So we find that f is completely determined if we know $f(1)$. If $f(1) = n$, then $f(m) = nm = f_n(m)$. Hence $f = f_n$ and all the homomorphisms of $\mathbb{Z}$ into $\mathbb{Z}$ are given by f_n, $n = 0, \pm 1, \pm 2, \ldots$

◊ **Exercise 6.1.6.** Find all homomorphisms from $(\mathbb{Z}_8, +)$ into $(\mathbb{Z}_6, +)$.

Solution. We have $\mathbb{Z}_8 = \langle [1] \rangle$. Let $f : \mathbb{Z}_8 \to \mathbb{Z}_6$ be a homomorphism. For any $[a] \in \mathbb{Z}_8$, $f([a]) = af([1])$ shows that f is completely known if $f([1])$ is known. Now $o(f[1])$ divides $o([1])$ and $|\mathbb{Z}_6|$, i.e., $o(f[1])$ divides 8 and 6. Hence, $o(f[1]) = 1$ or 2. Thus, $f([1]) = [0]$ or $[3]$. If $f([1]) = [0]$ then f is the trivial homomorphism which

maps every element to $[0]$. On the other hand, $f([1]) = [3]$ implies that $f([a]) = [3a]$ for all $[a] \in \mathbb{Z}_8$. Thus $f\big([a]+[b]\big) = f\big([a+b]\big) = [3(a+b)] = [3a+3b] = [3a]+[3b] = f([a]) + f([b])$, proving that the function $f : \mathbb{Z}_8 \to \mathbb{Z}_6$ defined by $f([a]) = [3a]$ for all $[a] \in \mathbb{Z}_8$ is a homomorphism. Hence there are two homomorphisms from $\mathbb{Z}_8$ into $\mathbb{Z}_6$.

◊ **Exercise 6.1.7.** Show that there does not exist any isomorphism from the group $(\mathbb{R}, +)$ to the group $(\mathbb{R}^*, \cdot)$.

Solution. Observe that 0 is the identity element of the group $(\mathbb{R}, +)$. Hence no nonzero element of $\mathbb{R}$ is of finite order. Now for the group $(\mathbb{R}^*, \cdot)$, 1 is the identity element and -1 is an element of order 2. So, if there exists an isomorphism $f : \mathbb{R} \to \mathbb{R}^*$, there should exist $a \in \mathbb{R}$ such that $o(a) = 2$. But this is not the case. Hence there is no isomorphism from the group $(\mathbb{R}, +)$ to the group $(\mathbb{R}^*, \cdot)$.

◊ **Exercise 6.1.8.** Show that $(\mathbb{Q}, +)$ is not isomorphic to $(\mathbb{Q}^+, \cdot)$.

Solution: Suppose $f : \mathbb{Q} \to \mathbb{Q}^+$ is an isomorphism of groups. Now $2 \in \mathbb{Q}^+$ Hence there exists $x \in \mathbb{Q}$ such that $2 = f(x) = f\left(\frac{x}{2} + \frac{x}{2}\right) = f\left(\frac{x}{2}\right) f\left(\frac{x}{2}\right) = f\left(\frac{x}{2}\right)^2$. But there is no rational number y such that $2 = y^2$. So, there does not exist any isomorphism between $(\mathbb{Q}, +)$ and $(\mathbb{Q}^+, \cdot)$.

Exercise

1. Which of the following functions $f : G \to G_1$ are homomorphisms of groups? In the cases where f is a homomorphism, determine its kernel.
   (a) $G = (\mathbb{R}^+, \cdot)$; $G_1 = (\mathbb{R}^+, \cdot)$; $f(a) = a^4$ for all $a \in \mathbb{R}^+$
   (b) $G = (\mathbb{R}, +)$; $G_1 = (\mathbb{R}^+, \cdot)$; $f(a) = 3^a$ for all $a \in \mathbb{R}$.
   (c) $G = (\mathbb{R}^*, \cdot)$; $G_1 = (\mathbb{R}^+, \cdot)$; $f(a) = |a|$ for all $a \in \mathbb{R}^*$
   (d) $G = (\mathbb{Z}, +)$; $G_1 = (\mathbb{Z}, +)$; $f(a) = a + 5$ for all $a \in \mathbb{Z}$.
   (e) $G = (\mathbb{R}^*, \cdot)$; $G_1 = GL(2, \mathbb{R})$; $f(a) = \begin{bmatrix} 1 & 0 \\ 0 & a \end{bmatrix}$ for all $a \in \mathbb{R}^*$
   (f) $G = GL(2, \mathbb{R})$; $G_1 = (\mathbb{R}, +)$; $f\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = a + d$ for all $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2, \mathbb{R})$. where $GL(2,\mathbb{R})$ be the group of all non-singular matrices over $\mathbb{R}$.
   (g) $G = (\mathbb{R}^*, \cdot)$; $G_1 = \{1, -1\}$; $f(a) = 1$ if $a > 0$ and $f(a) = -1$ if $a < 0$.
2. Show that the group $(\mathbb{Z}_6, +)$ is a homomorphic image of the group $(\mathbb{Z}, +)$.
3. Show that there exists a homomorphism from the group $\mathbb{Z}$ onto the group $\mathbb{Z}/5\mathbb{Z}$.

$$\begin{aligned}
\ker\psi &= \{a \in G \mid \psi(a) = \text{ identity element of } A(G)\} \\
&= \{a \in G \mid \psi(a) \text{ is the identity function on } G\} \\
&= \{a \in G \mid \psi(a)(e) = e\} \\
&= \{a \in G \mid \tau_a(e) = e\} \\
&= \{a \in G \mid ae = e\} \\
&= \{a \in G \mid a = e\} \\
&= \{e\}.
\end{aligned}$$

So it follows that ψ is a monomorphism. Since $Im\psi = \psi(G)$ is a subgroup of $A(G)$, therefore G is isomorphic to the subgroup $\psi(G)$ of $A(G)$. □

Corollary 6.1.19. *Let G be a group of order n. G is isomorphic to a subgroup of the symmetric group S_n.*

Proof. The permutation group $A(G)$ on elements of G is isomorphic to the group S_n. Hence the corollary follows from the theorem above. □

Worked Out Exercises

◊ **Exercise 6.1.1.** Which of the following functions $f : G \to G_1$ are homomorphisms of groups? Of the homomorphisms, which are epimorphisms; which are monomorphisms and which are isomorphisms?

(a) $G = (\mathbb{Z}, +)$; $G_1 = (\mathbb{Z}, +)$; $f(x) = 4x$

(b) $G = (\mathbb{Z}, +)$; $G_1 = (\mathbb{Z}, +)$; $f(x) = -x$

(c) $G = GL(2, \mathbb{R})$, $G_1 = (\mathbb{R}, +)$, $f\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = a + b + c + d$

(d) $G = \mathcal{S}_3$; $G_1 = \{1, -1\}$; $f(\sigma) = 1$ if σ is even and $f(\sigma) = -1$ if σ is odd.

Solution. (a) Let $a, b \in \mathbb{Z}$, $f(a + b) = 4(a + b) = 4a + 4b = f(a) + f(b)$. Hence f is a homomorphism. Now $3 \in \mathbb{Z}$, but there is no integer $n \in \mathbb{Z}$ such that $4n = 3$. Hence $f(n) \neq 3$ for any $n \in \mathbb{Z}$, whence f is not an epimorphism.

Let $a, b \in \mathbb{Z}$ such that $a \neq b$. Then $4a \neq 4b$. Hence $f(a) \neq f(b)$. Consequently, f is a monomorphism. Thus we see that f is a monomorphism but not an epimorphism and hence not an isomorphism.

(b) Let $a, b \in \mathbb{Z}$. Now $f(a + b) = -(a + b) = (-a) + (-b) = f(a) + f(b)$, whence f is a homomorphism. Let $b \in \mathbb{Z}$. Then $-b \in \mathbb{Z}$ and $f(-b) = -(-b) = b$, which shows that f is an epimorphism. Also $a \neq b$ implies that $-a \neq -b$ and so $f(a) \neq f(b)$, whence f is a monomorphism. Combining all these we find that f is an isomorphism.

(c) Let us consider $A = \begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$. Now $A, B \in GL(2, \mathbb{R})$ and $AB = \begin{bmatrix} 2 & 1 \\ 4 & 1 \end{bmatrix}$.

Then $f(AB) = 2+1+4+1 = 8$ but $f(A)+f(B) = (2+3+4+5)+(1+(-1)+0+1) = 14+1 = 15$. Hence $f(AB) \neq f(A)+f(B)$ and so f is not a homomorphism.

(d) Let $\sigma, \delta \in S_3$. If σ and δ are both even, then $\sigma\delta$ is even and hence $f(\sigma\delta) = 1 = 1 \cdot 1 = f(\sigma)f(\delta)$.

Suppose that σ is even and δ is odd. Then $\sigma\delta$ is odd and $f(\sigma\delta) = -1 = 1 \cdot (-1) = f(\sigma)f(\delta)$. Again if σ is odd and δ is even, then $\sigma\delta$ is odd and as above, we have $f(\sigma\delta) = f(\sigma)f(\delta)$.

Now suppose that both σ and δ are odd. Then $\sigma\delta$ is even and $f(\sigma\delta) = 1 = (-1)\cdot(-1) = f(\sigma)f(\delta)$. Hence f is a homomorphism.

Now (123) is an even permutation and (12) is an odd permutation. Then, $1 = f\big((123)\big)$ and $-1 = f\big((12)\big)$. Hence f is surjective and so f is an epimorphism. Now (123) and (132) are two distinct even permutations. But we find that $f\big((123)\big) = f\big((132)\big) = 1$, whence f is not injective and so f is not a monomorphism.

◊ **Exercise 6.1.2.** If a function $f : G \to G_1$ of Worked Out Exercise 6.1.1 above is a homomorphism, then find its kernel.

Solution. (a) Here f is a homomorphism.

$$\begin{aligned} \ker f &= \{n \in \mathbb{Z} \mid f(n) = \text{identity of the group } G_1\} \\ &= \{n \in \mathbb{Z} \mid f(n) = 0\} \\ &= \{n \in \mathbb{Z} \mid 4n = 0\} \\ &= \{0\}. \end{aligned}$$

(b) In this case also f is a homomorphism.

$$\begin{aligned} \ker f &= \{n \in \mathbb{Z} \mid f(n) = \text{identity of the group } G_1\} \\ &= \{n \in \mathbb{Z} \mid f(n) = 0\} \\ &= \{n \in \mathbb{Z} \mid -n = 0\} \\ &= \{0\}. \end{aligned}$$

(d) Again in this case f is a homomorphism.