Let a, b be any two elements of G then

$f(ab) = (ab)^{-1}$ [by defination of f]

$= (ba)^{-1}$ [$\because G$ is abelian]

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

$\therefore f$ is an automorphism of G.

Conversely → Suppose that f is an automorphism of G.

Let $a, b \in G$

we have $f(ab) = (ab)^{-1} = b^{-1}a^{-1} = f(b)\,f(a)$

$= f(ba)$ {$\because f$ is an automorphism}

Since f is one-one therefore

$f(ab) = f(ba)$

$\Rightarrow ab = ba \Rightarrow G$ is abelian

NOTE → $A(G)$ denote the set of all automorphism of G.

V.V.I.

Theorem → If G is a group then $A(G)$ the set of all automorphisms of G is also a group.

Ans → We have

$A(G) = \{f : f$ is an automorphism of $G\}$

Since the identity mapping $I : G \to G$ is an automorphism

Hence set $A(G)$ is non empty

(1) **Closure property** ÷ Let $f_1, f_2 \in A(G)$ then f_1, f_2 are one-one mapping of G on to itself.

$\therefore f_1 f_2$ is also one-one maping of G onto itself

If a, b be any two elements of G

We have,

$(f_1 f_2)(ab) = f_1[f_2(ab)] = f_1[f_2(a)\,f_2(b)]$

$= f_1[f_2(a)]\,f_1[f_2(b)]$

$= [(f_1 f_2)(a)]\,[(f_1 f_2)(b)]$

$\therefore f_1 f_2$ is also an automorphism of $A(G)$

$\Rightarrow f_1 f_2 \in A(G)$

Thus $A(G)$ is closed with respect to composite composition.

(ii) Associative property → We know that composite of arbitrary mapping is ~~also~~ associative. Therefore composite of automorphism is also associative.

(iii) Existence of identity :- The identity mapping $I: G \to G$ is an automorphism of G. I is obviously one-one onto and if $a, b \in G$

Then $I(ab) = ab = I(a)\, I(b)$

Thus $I \in A(G)$ and if $f \in A(G)$ we have

$$If = fI = f$$

(iv) Existence of inverse :- Let $f \in A(G)$. Since f is one one mapping G onto itself.

Therefore f^{-1} exists and is also one-one and onto of G

we shall show that f^{-1} is an automorphism of G.

Let $a, b \in G$ then $\exists\ a', b' \in G$, such that

$f(a) = a' \quad f(b) = b'$

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

We have

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

$= f^{-1}[f(ab)]$ [$\because f$ is an automorphism]

$= I(ab) = ab = f^{-1}(a')\, f^{-1}(b')$

$\therefore f^{-1}$ is an automorphism of G and thus

$f \in A(G) \Rightarrow f^{-1} \in A(G)$

$\therefore$ Each element of $A(G)$ is invertable.

Hence $A(G)$ is a group with respect to composit composition.

—x—

Note → $A(G)$ is not abelian, since, composition of mapping is not commutative.

IMP
Theorem → The set $I(G)$ of all Inner automorphism of a group G is a group.

Proof → The inner automorphism of the group G is defined by a mapping

$f_a : G \to G$ such that

$f_a(x) = a^{-1}xa, \ \forall x \in G$ and $a \in G$

$\therefore I(G) = \{f_a : f_a(x) = a^{-1}xa \ \forall x \in G, a \in G\}$

To prove that $I(G)$ is a group for which we verify the ~~ver~~ following group axioms.

(i) Closure property – Let ~~f(a), f(b) ∈ I(G) then~~ $f_a, f_b \in I(G)$

$$(f_a f_b)x = f_a\{f_b(x)\}$$
$$= f_a\{b^{-1}xb\}$$
$$= a^{-1}\{b^{-1}xb\}a$$
$$= a^{-1}b^{-1}xba$$
$$= (ba)^{-1}x(ba) = f_{ba}(x)$$

$\therefore f_a f_b = f_{ba}$

Since $a, b \in G \Rightarrow ab \in G \Rightarrow f_{ba} \in I(G) \Rightarrow f_a f_b \in I(G)$

This proves that closure property hold in $I(G)$.

(ii) Associative property → Let $f_a, f_b, f_c \in I(G)$.

We have to prove

$$f_a(f_b f_c) = (f_a f_b) f_c$$

L.H.S $= f_a(f_b f_c) = f_a f_{cb} = f_{(cb)a}$

and R.H.S $= (f_a f_b) f_c$ ~~= f_b f_c = f_c(ba)~~ $= (f_{ba}) f_c = f_{c(ba)}$

Since, $(cb)a = c(ba)$ hold in G $\{\because G$ is a group$\}$

$\Rightarrow f_a(f_b f_c) = (f_a f_b) f_c$

~~Since G is group.~~

$\therefore$ R.H.S = L.H.S

(iii) Existence of identity – If e be the identity element of G. Then f_e is the identity element of $I(G)$. Since

$$f_a f_e = f_{ea} = f_a = f_e f_a$$

(iv) Existence of inverse – Clearly, $f_{a^{-1}}$ is the inverse of $f_a \in I(G)$,

Since $f_{a^{-1}} f_a = f_{aa^{-1}} = f_e$

and, $f_a f_{a^{-1}} = f_{a^{-1}a} = f_e$

$\therefore I(G)$ is a group.

PERMUTATION –

Definition – A one-one maping of a finite set onto itself is called a permutation i.e $f: G \to G$ is called a permutation if f is one-one and onto. The no. of elements in the set G is called the degree of permutation.

Symmetric set → The set of all permutations of a given set G of n elements is denoted by P_n which will have $\lfloor n$ permutations. It is called a symmetric set of degree n.

Note → If $(a_1, a_2, \ldots, a_n)$ be n distinct elements of a set G then the operation of replacing a_1 by b_1, a_2 by b_2 ... a_n by b_n be expressed as.

$$P = \begin{bmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{bmatrix}$$