12 Notranji automorfizem. Grupa automorfizmov.

Spomnimo se: Preslikava ϕ iz grupe G sama vase se imenuje automorfizem grupe G če in samo če (i) $\phi(ab) = \phi(a)\phi(b)$ za $\forall a, b \in G$; (ii) ϕ je injekcija; (iii) ϕ je surjekcija.

Izrek
Naj bo f automorfizem grupe G. Če je N edinka grupe G, potem je $f(N)$ tudi edinka grupe G.

1. Dokaži izrek zgoraj.

2. Naj bo G grupa in naj bo Z center grupe G. Če je f automorfizem grupe G, pokaži da je potem $f(Z) \subseteq Z$.

3. Naj bo G grupa in naj bo f automorfizem grupe G. Če za $a \in G$ definiramo $N(a) = \{x \in G : ax = xa\}$, pokaži da potem velja $N(f(a)) = f(N(a))$.

4. Naj bo G grupa in naj bo a poljubni ampak fiksen element grupe G. Naj bo f_a preslikava iz G v G definirana z $f_a(x) = a^{-1}xa$, $x \in G$. Pokaži, da je preslikava f_a dobro definirana in da je automorfizem grupe G.

Definicija (notranji in zunanji automorfizem)
Naj bo $a \in G$. Automorfizem $f_a(x) = a^{-1}xa$, $x \in G$, se imenuje notranji automorfizem grupe G, ki ustreza elementu a. Automorfizem, ki ni notranji automorfizem, se imenuje zunanji automorfizem.

5. Naj bo G aditivna grupa celih števil. Poišči notranji automorfizem grupe G, ki ustreza elementu 5 grupe G.

6. Poišči zgled grupe G v kateri obstajata elementa $a, b \in G$, $a \neq b$, tako da velja $f_a = f_b$ (f_a in f_b sta dva notranja automorfizma grupe G, tako da $f_a = f_b$).

7. Naj bo $f : G \to G$ homomorfizem in naj f komutira z vsakim notranjim automorfizmom grupe G. Pokaži da je $H = \{x \in G : f^2(x) = f(x)\}$ edinka grupe G.

Izrek
Za abelske grupe je edini notranji automorfizem identična preslikava, medtem ko za neabelske grupe obstaja netrivialen notranji automorfizem.

8. Dokaži izrek zgoraj.

9. Naj bo G grupa in naj bo $\mathrm{Aut}(G)$ množica vseh automorfizmov grupe G. Pokaži, da je množica $\mathrm{Aut}(G)$ grupa glede na operacijo kompozicije funkcij.

Definicija (grupa automorfizmov)
Grupo $\mathrm{Aut}(G)$, vseh automorfizmov grupe G, glede na operacijo kompozicije funkcij, imenujemo grupa automorfizmov grupe G.

10. Naj bo G ciklična grupa reda 4. Pokaži, da je grupa automorfizmov grupe G, reda 2.

11. Če je $|\mathrm{Aut}(G)| > 1$, pokaži da je potem $|G| > 2$.

12. Naj bo G neskončna ciklična grupa. Pokaži, da je $|\mathrm{Aut}(G)| = 2$.

13. Naj bo G končna ciklična grupa reda n. Pokaži, da je potem $|\mathrm{Aut}(G)| = \phi(n)$, kjer je ϕ Eulerjeva funkcija fi.

14. Naj bo G grupa in naj bo $\mathrm{Inn}(G)$ množica notranjih automorfizmov grupe G. Pokaži, da je množica $\mathrm{Inn}(G)$ grupa glede na operacijo kompozicije.

Definicija (Inn(G))
Grupo Inn(G) vseh notranjih automorfizmov grupe G, glede na operacijo kompozicije, imenujemo grupa notranjih automorfizmov grupe G.

15. Določi Inn(D_4) (po potrebi uporabi Cayley-evo tabelo, ki smo jo imeli v eni od prejšnjih nalog).

16. Določi Aut($\mathbb{Z}_{10}$).

17. Pokaži, da je Aut($\mathbb{Z}_n$) $\cong U(n)$.

Izrek
Množica Inn(G) vseh notranji automorfizmov grupe G je edinka grupe Aut(G) vseh automorfizmov grupe G.

18. Dokaži izrek zgoraj.

Izrek (Inn(G) $\cong G/Z(G)$)
Za vsako grupo G, je $G/Z(G)$ izomorfna z Inn(G).

19. Dokaži izrek zgoraj.

20. Naj bo $G = S_3$. Pokaži, da je Inn(G) $\cong G$.

POMEMBNI REZULTATI

1. Naj bo f automorfizem grupe G. Če je H podgrupa grupe G, potem je $f(H)$ tudi podgrupa grupe G.
2. Naj bo f automorfizem grupe G. Če je N edinka grupe G, potem je $f(N)$ tudi edinka grupe G.
3. Za abelske grupe je edini notranji automorfizem identična preslikava, medtem ko za neabelske grupe obstaja netrivialen notranji automorfizem.
4. Množica Inn(G) vseh notranjih automorfizmov grupe G je edinka grupe Aut(G) (vseh automorfizmov grupe G).
5. Za vsako grupo G je $G/Z(G)$ izomorfna z Inn(G) (kjer je $Z(G)$ center grupe G).

Let $f(n_1), f(n_2) \in f(N)$

Now $f(n_1)(f(n_2))^{-1} = f(n_1)f(n_2^{-1}) = f(n_1 n_2^{-1}) \in f(N)$

$(\because \quad n_1, n_2 \in N \Rightarrow n_1 n_2^{-1} \in N)$

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

Let $f(n) \in f(N)$ and $g \in G$. Since f is onto, there exists $x \in G$ such that $g = f(x)$.

Now $gf(n)g^{-1} = f(x)f(n)(f(x))^{-1} = f(x)f(n)f(x^{-1}) = f(xnx^{-1}) \in f(N)$

$(\because \quad n \in N, x \in G \Rightarrow xnx^{-1} \in N)$

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

Example 8. *Let G be a group and Z, the centre of G. If f is any automorphism of G, show that* $f(Z) \subseteq Z$.

Sol. We have $Z = \{z \in G : zx = xz \ \forall\, x \in G\}$.

Let $f(z) \in f(Z)$. Let x be any element of G. Since f is onto, there exists $y \in G$ such that $f(y) = x$.

Now $f(z) \in f(Z) \Rightarrow z \in Z$

$\Rightarrow$ $zy = yz \Rightarrow f(zy) = f(yz)$

$\Rightarrow$ $f(z)f(y) = f(y)f(z) \Rightarrow f(z)x = xf(z)$

$\therefore$ $f(z) \in Z \quad \therefore \quad f(Z) \subseteq Z$.

Example 9. *Let G be a group and f, an automorphism of G. If for* $a \in G$, $N(a) = \{x \in G : ax = xa\}$, *show that* $N(f(a)) = f(N(a))$.

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

$\therefore$ $N(f(a)) = \{x \in G : f(a)x = xf(a)\}$

Let $x \in N(f(a))$.

$\Rightarrow$ $f(a)x = xf(a) \Rightarrow f(a)f(y) = f(y)f(a)$ (Taking $x = f(y), y \in G$)

$\Rightarrow$ $f(ay) = f(ya) \Rightarrow ay = ya$ ($\because$ f is one-one)

$\Rightarrow$ $y \in N(a) \Rightarrow f(y) \in f(N(a))$ *i.e.*, $x \in f(N(a))$

$\therefore$ $N(f(a)) \subseteq f(N(a))$.

Now, let $b \in f(N(a)) \quad \therefore \quad \exists\, c \in N(a) : f(c) = b$

$c \in N(a) \Rightarrow ac = ca$

$\Rightarrow$ $f(ac) = f(ca) \Rightarrow f(a)f(c) = f(c)f(a)$

$\Rightarrow$ $f(a)b = bf(a) \Rightarrow b \in N(f(a))$

$\therefore$ $f(N(a)) \subseteq N(f(a))$.

Combining, we get $N(f(a)) = f(N(a))$.

3. INNER AUTOMORPHISM

Let G be a group and let a be any arbitrary but fixed element of G.

Let f_a be a mapping from G into G defined by $f_a(x) = a^{-1}xa, \quad x \in G$.

f_a is well defined. Let $x, y \in G$.

$$x = y \Rightarrow a^{-1}xa = a^{-1}ya \Rightarrow f_a(x) = f_a(y)$$

$\therefore$ f_a is well defined.

f_a is a homomorphism. Let $x, y \in G$.

$$f_a(xy) = a^{-1}(xy)a = a^{-1}(x(aa^{-1})y)a = (a^{-1}xa)(a^{-1}ya) = f_a(x)\,f_a(y)$$

$\therefore$ f_a is a homomorphism.

f_a is one-one. Let $x, y \in G$.

$f_a(x) = f_a(y) \Rightarrow a^{-1}xa = a^{-1}ya \Rightarrow a(a^{-1}xa)a^{-1} = a(a^{-1}ya)a^{-1}$

$\Rightarrow (aa^{-1})x(aa^{-1}) = (aa^{-1})y(aa^{-1}) \Rightarrow exe = eye \Rightarrow x = y.$

$\therefore$ f_a is one-one.

f_a is onto. Let $x \in G$.

$\therefore$ $axa^{-1} \in G$ and

$f_a(axa^{-1}) = a^{-1}(axa^{-1})a = (a^{-1}a)x(a^{-1}a) = exe = x$

$\therefore$ Given $x \in G, \exists\, axa^{-1} \in G : f_a(axa^{-1}) = x.$

$\therefore$ f_a is onto.

$\therefore$ f_a is an automorphism of G.

For $a \in G$, the automorphism $f_a(x) = a^{-1}xa, x \in G$ is called an **inner automorphism** of the group G corresponding to the element a.

An automorphism which is not an inner automorphism is called an **outer automorphism.**

Example 10. *Let G be the additive group of the integers. Find the inner automorphism of G corresponding to the element 5 of G.*

Sol. The inner automorphism f_a of group G corresponding to the element a of G is defined as $f_a(x) = a^{-1}xa \ \forall\, x \in G$.

In this particular case, the binary operation is '+'.

$\therefore$ $f_5(x) = (-5) + x + 5 \quad \forall\, x \in G$

i.e., $\mathbf{f_5(x) = x \quad \forall\, x \in G.}$

Example 11. *Give an example of a group in which the inner automorphism corresponding to two distinct elements of the group may be same.*

Sol. Let $G = \{1, -1, i, -i\}$. G is a group with usual multiplication as the binary operation.

$1 \in G$ and $f_1(x) = (1)^{-1}x(1) \quad \forall\, x \in G$

$\therefore$ $f_1(x) = (1)x(1) = x \quad \forall\, x \in G$

Also, $-1 \in G$ and $f_{-1}(x) = (-1)^{-1}(x)(-1) \quad \forall\, x \in G$

$\therefore$ $f_{-1}(x) = (-1)x(-1) = x \quad \forall\, x \in G$

$\therefore$ $f_1 = f_{-1}$.

Example 12. *Let $f : G \to G$ be a homomorphism. Let f commute with every inner automorphism of G. Show that $H = \{x \in G : f^2(x) = f(x)\}$ is a normal subgroup of G.*

Sol. We have

$H = \{x \in G : f^2(x) = f(x)\}$

$f^2(e) = f(f(e)) = f(e) \Rightarrow e \in H \quad \therefore \quad H \neq \phi$

Let $a, b \in H \quad \therefore \quad f^2(a) = f(a), f^2(b) = f(b).$

Now $f^2(ab) = f(f(ab)) = f(f(a)f(b))$

$= f(f(a))f(f(b))$ ($\because$ f is a hom.)

$= f^2(a)f^2(b) = f(a)f(b) = f(ab).$

$\therefore$ $ab \in H$

Also, $f^2(a^{-1}) = f(f(a^{-1})) = f((f(a))^{-1}) = (f(f(a)))^{-1} = (f^2(a))^{-1} = (f(a))^{-1} = f(a^{-1}).$

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

$\therefore$ H is a subgroup of G. Let $x \in G, h \in H$.

$\therefore \quad f^2(xhx^{-1}) = f(f(xhx^{-1})) = f(f(f_{x^{-1}}(h))) \qquad (\because f_{x^{-1}}(h) = (x^{-1})^{-1} hx^{-1} = xhx^{-1})$

$= f((ff_{x^{-1}})(h)) = f((f_{x^{-1}}f)(h))$

$= f(f_{x^{-1}}(f(h))) = f((x^{-1})^{-1} f(h)\, x^{-1})$

$= f(xf(h)\, x^{-1}) = f(x)\, f(f(h))\, f(x^{-1})$

$= f(x)\, f^2(h)\, f(x^{-1}) = f(x)\, f(h)\, f(x^{-1}) = f(xhx^{-1})$

$\therefore \quad xhx^{-1} \in H.$

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

Theorem 1. *For an abelian group, the only inner automorphism is the identity mapping whereas for non-abelian groups there exists non-trivial inner automorphisms.*

Proof. Let G be an abelian group and $a \in G$.

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

$\Rightarrow \quad f_a(x) = a^{-1}(ax) = (a^{-1}a)x = ex = x \quad \forall\, x \in G. \quad \therefore \quad f_a$ is the identity mapping of G.

$\therefore$ In an abelian group, the only inner automorphism is the identity mapping.

Let G be a non-abelian group.

$\therefore$ There exists at least two elements a and b in G such that $ab \neq ba$.

$\Rightarrow \quad b^{-1}(ab) \neq b^{-1}(ba) \quad \Rightarrow \quad b^{-1}ab \neq (b^{-1}b)\, a \quad \Rightarrow \quad b^{-1}ab \neq a$

$\Rightarrow \quad f_b(a) \neq a. \quad \therefore \quad f_b$ is not the identity mapping of G.

$\therefore$ For non-abelian groups, there exists non-trivial inner automorphisms.

4. GROUP OF AUTOMORPHISMS

Let G be a group and let A(G) be the set of all automorphisms of G. We shall show that the set A(G) is a group with respect to composition of functions as the binary operation.

Let $f, g \in A(G)$.

For $x \in G$, $(fg)^*(x) = f(g(x)) \in G$

$\therefore$ fg is a mapping from G to G. Let $x, y \in G$.

$\therefore \quad (fg)(xy) = f(g(xy)) = f(g(x)\, g(y)) = f(g(x))\, f(g(y)) = (fg)(x)(fg)(y)$

$\therefore$ fg is a homomorphism.

Let $x, y \in G$ and $(fg)(x) = (fg)(y)$.

$\Rightarrow \quad f(g(x)) = f(g(y)) \quad \Rightarrow \quad g(x) = g(y) \qquad (\because f$ is one-one)

$\Rightarrow \quad x = y. \qquad (\because g$ is one-one)

$\therefore$ fg is one-one.

Let $x \in G$. Since f is onto, $\quad \exists\, y \in G : f(y) = x.$

Also, $y \in G$ and g is onto, so $\quad \exists\, z \in G : g(z) = y.$

$\therefore \quad x = f(y) = f(g(z)) = (fg)(z)$

$\therefore$ Given $\quad x \in G, \exists\, z \in G : (fg)(z) = x.$

$\therefore$ fg is onto.

$\therefore$ fg is an automorphism of the group G *i.e.*, $fg \in A(G)$.

$\therefore$ Composition of functions is a binary operation on A(G).

Associativity. Let $f, g, h \in A(G)$.

For $\quad x \in G, \quad (f(gh))(x) = f(gh(x)) = f(g(h(x)))$

*For the sake of simplicity, we have written fog as fg.

Also $((fg)h)(x) = (fg)(h(x)) = f(g(h(x))$

$\therefore$ $(f(gh))(x) = ((fg)h)(x), \quad \forall\, x \in G$

$\therefore$ $f(gh) = (fg)h \quad \forall\, f, g, h \in A(G).$

Existence of identity. Let the identity function on G be denoted by i.

$\therefore$ i is one-one onto.

Also, for $x, y \in G$, we have $i(xy) = xy = i(x)\, i(y)$.

$\therefore$ i is an automorphism of G *i.e.*, $i \in A(G)$.

Also, for $f \in A(G)$,

$$(fi)(x) = f(i(x)) = f(x) \quad \text{and} \quad (if)(x) = i(f(x)) = f(x)$$

$\therefore$ $(fi)(x) = f(x) = (if)(x) \quad \forall\, x \in G$

$\therefore$ $fi = f = if \quad \forall\, f \in A(G).$

$\therefore$ 'i' is the identity of A(G).

Existence of inverse. Let $f \in A(G)$

$\therefore$ f is one-one mapping of G onto G.

$\therefore$ f^{-1} exists and is also one-one onto.

Let $x, y \in G$.

Let $f^{-1}(x) = x'$ and $f^{-1}(y) = y'$.

$\therefore$ $f(x') = x$ and $f(y') = y$

$\therefore$ $f^{-1}(xy) = f^{-1}(f(x')\, f(y')) = f^{-1}(f(x'y')) = (f^{-1}f)(x'y') = i(x'y') = x'y' = f^{-1}(x)\, f^{-1}(y)$.

$\therefore$ f^{-1} is a homomorphism.

$\therefore$ f^{-1} is an automorphism of G *i.e.*, $f^{-1} \in A(G)$.

Also $ff^{-1} = i = f^{-1}f$

$\therefore$ f^{-1} is the inverse of f.

$\therefore$ A(G) is a group with composition of mappings as the binary operation. The group A(G) is called the **group of automorphisms** of the group G.

Example 13. *Let G be a cyclic group of order 4. Show that the group of automorphisms of G is of order 2.*

Sol. Let $G = \{e, a, a^2, a^3\}$, where $a^4 = e$.

$\therefore$ $o(e) = 1, o(a) = 4, o(a^2) = 2, o(a^3) = 4$

$(\because \quad (a^2)^2 = a^4 = e\,;\, a^3 \neq e, (a^3)^2 = a^6 = a^2 \neq e, (a^3)^3 = a^9 = a \neq e, (a^3)^4 = a^{12} = e)$

Let f be an automorphism of G.

$\therefore$ $o(f(b)) = o(b)\ \forall\, b \in G$

$\Rightarrow$ $f(a) = a$ or a^3 $\qquad (\because \quad o(a) = o(a^3) = 4)$

$f(a^2) = a^2$ $\qquad (\because$ There is only one element of order 2)

$f(a^3) = a$ or a^3

$f(a^4) = e$

Since an automorphism is also 1 – 1 and onto, we have only two possible automorphisms, say ϕ and Ψ defined as :

$$\phi(e) = e, \phi(a) = a, \phi(a^2) = a^2, \phi(a^3) = a^3,$$

and $$\Psi(e) = e, \Psi(a) = a^3, \Psi(a^2) = a^2, \Psi(a^3) = a.$$

$\therefore$ $o(A(G)) = 2.$

5. CHARACTERISTIC SUBGROUP

A subgroup H of a group G is called a characteristic subgroup of the group G if $f(H) \subseteq H \ \forall f \in A(G)$.

Example 14. *Let* $G = \{e, a, a^2, a^3\}$ *be a cyclic group of order 4. Show that* $H = \{e, a^2\}$ *is a characteristic subgroup of G.*

Sol. Since G is a cyclic group of order 4, we have $A(G) = \{\phi, \Psi\}$, where

$$\phi(e) = e, \ \phi(a) = a, \ \phi(a^2) = a^2, \ \phi(a^3) = a^3$$

and $$\Psi(e) = e, \Psi(a) = a^3, \Psi(a^2) = a^2, \Psi(a^3) = a.$$

$\therefore$ $$\phi(H) = \{\phi(e), \phi(a^2)\} = \{e, a^2\} = H.$$

and $$\Psi(H) = \{\Psi(e), \Psi(a^2)\} = \{e, a^2\} = H.$$

$\therefore$ H is a characteristic subgroup of G.

Example 15. *Show that every subgroup of a finite cyclic group is a characteristic subgroup.*

Sol. Let $G = (a)$ be a finite cyclic group of order n.

$\therefore$ $$G = \{a^0 (= e), a, a^2, \ldots\ldots, a^{n-1}\}$$

Let H be any subgroup of G.

$\therefore$ $H = (a^m)$ for some integer m, where $0 \le m \le n$. Let f be any automorphism of G.

$\therefore$ $f(a) \in G$. Let $f(a) = a^k$ for some k such that $0 \le k \le n$.

Let $h \in H$. $\therefore$ $h = (a^m)^l$ for some integer l

Now
$$f(h) = f((a^m)^l) = f(a^{ml})$$
$$= (f(a))^{ml} = (a^k)^{ml} = a^{kml}$$
$$= (a^m)^{kl} \in H$$

$\therefore$ $f(h) \in H \ \forall f \in A(G), h \in H$

$\therefore$ H is a characteristic subgroup of G.

Example 16. *Show that a characteristic subgroup of a group G is a normal subgroup of G.*

Sol. Let H be a characteristic subgroup of group G.

$\therefore$ H is a subgroup of G and

$$f(H) \subseteq H \ \forall f \in A(G).$$

$\Rightarrow$ $$f(h) \in H \ \forall f \in A(G) \text{ and } h \in H \qquad \ldots(1)$$

Let $$h \in H \text{ and } g \in G.$$

$\therefore$ $$ghg^{-1} = (g^{-1})^{-1} hg^{-1} = f_{g^{-1}}(h),$$

where $f_{g^{-1}}$ is the inner automorphism of G corresponding to g^{-1}.

$\therefore$ Using (1), $f_{g^{-1}}(h) \in H$

$\Rightarrow$ $$ghg^{-1} \in H \ \forall h \in H \text{ and } g \in G$$

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

Example 17. *Let S be the conjugate class of a non-trivial element of a group G. Let* $\phi \in A(G)$. *Show that* $\phi(S)$ *is the conjugate class of some element of G.*

Sol. Let S be the conjugate class of $a(\neq e) \in G$.

$\therefore$ $$S = \{x^{-1}ax : x \in G\}.$$

$\therefore$ $$\phi(S) = \{\phi(x^{-1}ax) : x \in G\}$$

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

$\therefore$ $\phi(x^{-1}ax)$ is a conjugate of $\phi(a)$, because $\phi(x) \in G$.

$\therefore$ $\phi(S)$ is the conjugate class of non-trivial element $\phi(a)$ of G.

$(\phi(a)) = e \Rightarrow \phi(a) = \phi(e) \Rightarrow a = e$, which is not true.)

Example 18. *If $o(A(G)) > 1$, then show that $o(G) > 2$.*

Sol. If possible, let $o(G) \leq 2$.

Case I. $o(G) = 1$.

Here G has only one automorphism, namely the identity map on G.

$\therefore$ $o(A(G)) = 1$, which is impossible.

$\therefore$ $o(G) \neq 1$.

Case II. $o(G) = 2$.

Let $G = \{e, a\}$, where $a \neq e$ and $a^2 = a.a = e$. $(\because a^2 = a \Rightarrow a = e)$

Since $o(A(G)) > 1$, there exists a non-identity element, say f in A(G).

$\therefore$ $f(a) \neq a$ $(\because f(e) = e)$

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

$\therefore$ f is the identity automorphism. This is also impossible.

$\therefore$ $o(G) \neq 2$.

$\therefore$ Our supposition is wrong.

$\therefore$ $o(G) > 2$.

Example 19. *Let G be an infinite cyclic group. Show that $o(A(G)) = 2$.*

Sol. Let $G = (a)$.

$\therefore$ $G = \{a^0 (= e), a^{\pm 1}, a^{\pm 2}, a^{\pm 3}, \ldots\ldots\}$ and $a^i = e$ iff $i = 0$.

Let $f \in A(G)$

$\therefore$ $f(a^k) = (f(a))^k$ for $k \in Z$

$\therefore$ f is completely known, if we know $f(a)$.

Let $f(a) = a^m \in G$, where m is some integer.

Since f is onto and $a \in G$, there exist $a^\mu \in G$ such that $f(a^\mu) = a$.

$\therefore$ $a = f(a^\mu) = (f(a))^\mu = (a^m)^\mu = a^{m\mu}$

$\Rightarrow$ $a^{m\mu} = a \Rightarrow a^{m\mu} a^{-1} = aa^{-1} \Rightarrow a^{m\mu - 1} = e$

$\Rightarrow m\mu - 1 = 0 \Rightarrow m\mu = 1$

$\therefore$ $m = 1, \mu = 1$ or $m = -1, \mu = -1$

$\therefore$ $f(a) = a^1 = a$ or $f(a) = a^{-1}$

$\therefore$ There are only two automorphisms of the group G.

$\therefore$ $A(G) = 2$.

Example 20. *Let G be a finite cyclic group of order n. Show that $o(A(G)) = \phi(n)$, where ϕ is the Euler's function.*

Sol. Let $G = (a)$.

$\therefore$ $o(a) = n$ and $G = \{a^0 (= e), a^1, a^2, \ldots\ldots, a^{n-1}\}$

Let $f \in A(G)$

$\therefore$ $f(a^k) = (f(a))^k$ for $k \in Z$

$\therefore$ f is completely known, if we know $f(a)$.

Let $f(a) = a^m \in G$, where m is some integer such that $0 \leq m < n$.

Since f is an automorphism,

$(f(a))^n = f(a^n) = f(e) = e$.

$\therefore \quad o(f(a)) \le n$

If possible, let $o(f(a)) = \lambda, \quad 0 \le \lambda < n$

$\therefore \quad (f(a))^{\lambda} = e \quad \text{or} \quad f(a^{\lambda}) = f(e) \quad \text{or} \quad a^{\lambda} = e$

$\therefore$ $o(a) < n$, which is impossible.

$\therefore \quad o(f(a)) = n$

Let $(m, n) = d$, where $d \ge 1$. Let $d > 1$.

$\therefore \quad (f(a))^{n/d} = (a^m)^{n/d} = (a^n)^{m/d} = (e)^{m/d} = e$

$\therefore$ $o(f(a)) < n$, which is impossible. $(\because \ n/d < n)$

$\therefore$ d cannot be greater than 1 and we have $d = 1$ *i.e.*, $(m, n) = 1$

$\therefore$ If $f \in A(G)$, then $f(a) = a^m$, where $(m, n) = 1$.

$\therefore \quad o(A(G)) = \phi(n)$.

Theorem 1. *The set I(G) of all inner automorphisms of a group G is a normal subgroup of the group A(G) of automorphisms of G.*

Proof. The elements of I(G) are also automorphisms of the group G.

$\therefore \quad I(G) \subseteq A(G)$

The identity mapping (i) of G is an inner automorphism of G because for $x \in G$

$$i(x) = x = e^{-1}xe = f_e(x). \quad \therefore \quad I(G) \ne \phi.$$

Let $f_a, f_b \in I(G)$.

For $x \in G$, $(f_b f_{b^{-1}})(x) = f_b(f_{b^{-1}}(x)) = f_b((b^{-1})^{-1} x b^{-1}) = f_b(bxb^{-1})$

$$= b^{-1}(bxb^{-1})\, b = (b^{-1}b)\, x\, (b^{-1}b) = exe = x = i(x)$$

Also $(f_{b^{-1}} f_b)(x) = f_{b^{-1}}(f_b(x)) = f_{b^{-1}}(b^{-1}xb) = (b^{-1})^{-1}(b^{-1}xb)(b^{-1})$

$$= (bb^{-1})\, x\, (bb^{-1}) = exe = x = i(x)$$

$\therefore \quad (f_b f_{b^{-1}})(x) = i(x) = (f_{b^{-1}} f_b)(x) \ \forall \ x \in G$

$\Rightarrow \quad f_b f_{b^{-1}} = i = f_{b^{-1}} f_b \ \Rightarrow \ (f_b)^{-1} = f_{b^{-1}}$.

Now for $x \in G$,

$$(f_a(f_b)^{-1})(x) = (f_a f_{b^{-1}})(x) = f_a(f_{b^{-1}}(x)) = f_a((b^{-1})^{-1} x\, b^{-1}) = f_a(bxb^{-1})$$

$$= a^{-1}(bxb^{-1})\, a = (a^{-1}b)\, x\, (b^{-1}a) = (b^{-1}a)^{-1} x\, (b^{-1}a) = f_{b^{-1}a}(x)$$

$\therefore \quad (f_a(f_b)^{-1})(x) = f_{b^{-1}a}(x) \ \forall \ x \in G$

$\therefore \quad f_a(f_b)^{-1} = f_{b^{-1}a}$

$\therefore \quad f_a(f_b)^{-1} \in I(G) \qquad (\because \ a, b \in G \Rightarrow b^{-1}a \in G \Rightarrow f_{b^{-1}a} \in I(G))$

$\therefore$ I(G) is a subgroup of A(G).

Let $f_a \in I(G)$ and $f \in A(G)$.

For $x \in G$, $(ff_a f^{-1})(x) = (ff_a)(f^{-1}(x)) = f(f_a(f^{-1}(x)))$

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

$$= f(a^{-1})x\, f(a) = (f(a))^{-1} x\, f(a) = f_{f(a)}(x). \qquad (\because \ ff^{-1} = i)$$

$\therefore \quad ff_a f^{-1} = f_{f(a)}$

$\therefore \quad ff_a f^{-1} \in I(G) \qquad (\because \ f(a) \in G \Rightarrow f_{f(a)} \in I(G))$

$\therefore$ I(G) is a normal subgroup of A(G).

Theorem 2. *If I(G) is the set of all inner automorphisms of a group G and Z its centre, then* $I(G) \cong G/Z$. (K.U. 2005 ; M.D.U. 2005)

Proof. We know that I(G) is a subgroup of the group A(G).

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

Define $\phi : G \to I(G)$ by $\phi(a) = f_{a^{-1}}$, $a \in G$.

For $a, b \in G$, $\phi(ab) = f_{(ab)^{-1}} = f_{b^{-1}a^{-1}} = f_{a^{-1}} f_{b^{-1}} = \phi(a)\,\phi(b)$, because

$$f_{b^{-1}a^{-1}}(x) = (b^{-1}a^{-1})^{-1}\, x(b^{-1}a^{-1}) = ((a^{-1})^{-1}(b^{-1})^{-1})\, x(b^{-1}a^{-1}) = (a^{-1})^{-1}((b^{-1})^{-1}xb^{-1})a^{-1}$$

$$= f_{a^{-1}}((b^{-1})^{-1}xb^{-1}) = f_{a^{-1}}(f_{b^{-1}}(x)) = (f_{a^{-1}} f_{b^{-1}})(x) \quad \forall\, x \in G.$$

$\therefore$ ϕ is a homomorphism.

Let $f_t \in I(G)$ $\therefore$ $t, t^{-1} \in G$ and by definition of ϕ, we have $\phi(t^{-1}) = f_{(t^{-1})^{-1}} = f_t$.

$\therefore$ ϕ is also onto.

$\therefore$ By the **Fundamental theorem of homomorphism**, $G/\ker \phi \cong I(G)$.

We shall show that $\ker \phi = Z$. $x \in \ker \phi \Leftrightarrow \phi(x) = i \Leftrightarrow f_{x^{-1}} = f_e$ $(\because\ i = f_e)$

$\Leftrightarrow$ $f_{x^{-1}}(y) = f_e(y)\ \forall\, y \in G \Leftrightarrow (x^{-1})^{-1} y x^{-1} = e^{-1} y e\ \forall\, y \in G$

$\Leftrightarrow$ $(xyx^{-1})x = yx\ \forall\, y \in G \Leftrightarrow xy = yx\ \forall\, y \in G \Leftrightarrow x \in Z$.

$\therefore$ $\ker \phi = Z$.

$\therefore$ $G/Z \cong I(G)$ *i.e.,* $\mathbf{I(G) \cong G/Z}$.

Example 21. *If* $G = S_3$, *show that* $I(G) \cong G$.

Sol. We have $G = S_3$ and S_3 is the set of all one-to-one mappings of the set $\{a, b, c\}$ onto itself.

$\therefore$ $S_3 = \{I, (a\ b), (b\ c), (a\ c), (a\ b\ c), (a\ c\ b)\}$

We have already seen that the centre Z of S_3 is $\{I\}$.

Also, $I(G) \cong G/Z$

$\therefore$ $I(G) \cong G/\{I\}$

$\therefore$ $I(G) \cong G$ because $G/\{I\} \cong G$.

Remark : For the above group, we have

$$I(G) = \{f_1, f_{(a\ b)}, f_{(b\ c)}, f_{(a\ c)}, f_{(a\ b\ c)}, f_{(a\ c\ b)}\}.$$

IMPORTANT RESULTS

1. *Let f be an automorphism of a group G. If H is a subgroup of group G, then f(H) is also a subgroup of G.*
2. *Let f be an automorphism of a group G. If N is a normal subgroup of group G, then f(N) is also a normal subgroup of G.*
3. *For an abelian group, the only inner automorphism is the identity mapping whereas for non-abelian groups there exists non-trivial inner automorphisms.*
4. *The set I(G) of all inner automorphism of a group G is a normal subgroup of the group A(G) of automorphisms of G.*
5. *If I(G) is the set of all inner automorphisms of a group G and Z its centre, then* $I(G) \cong G/Z$.

The determination of Inn(G) is routine. If $G = \{e, a, b, c, \ldots\}$, then Inn($G$) $= \{\phi_e, \phi_a, \phi_b, \phi_c, \ldots\}$. This latter list may have duplications, however, since ϕ_a may be equal to ϕ_b even though $a \neq b$ (see Exercise 43). Thus, the only work involved in determining Inn(G) is deciding which distinct elements give the distinct automorphisms. On the other hand, the determination of Aut(G) is, in general, quite involved.

▮ EXAMPLE 12 Inn(D_4)

To determine Inn(D_4), we first observe that the complete list of inner automorphisms is ϕ_{R_0}, $\phi_{R_{90}}$, $\phi_{R_{180}}$, $\phi_{R_{270}}$, ϕ_H, ϕ_V, ϕ_D, and $\phi_{D'}$. Our job is to determine the repetitions in this list. Since $R_{180} \in Z(D_4)$, we have $\phi_{R_{180}}(x) = R_{180}xR_{180}^{-1} = x$, so that $\phi_{R_{180}} = \phi_{R_0}$. Also, $\phi_{R_{270}}(x) = R_{270}xR_{270}^{-1} = R_{90}R_{180}xR_{180}^{-1}R_{90}^{-1} = R_{90}xR_{90}^{-1} = \phi_{R_{90}}(x)$. Similarly, since $H = R_{180}V$ and $D' = R_{180}D$, we have $\phi_H = \phi_V$ and $\phi_D = \phi_{D'}$. This proves that the previous list can be pared down to ϕ_{R_0}, $\phi_{R_{90}}$, ϕ_H, and ϕ_D. We leave it to the reader to show that these are distinct (Exercise 13). ▮

EXAMPLE 13 Aut(Z_{10})

To compute Aut(Z_{10}), we try to discover enough information about an element α of Aut(Z_{10}) to determine how α must be defined. Because Z_{10} is so simple, this is not difficult to do. To begin with, observe that once we know $\alpha(1)$, we know $\alpha(k)$ for any k, because

$$\alpha(k) = \underbrace{\alpha(1 + 1 + \cdots + 1)}_{k \text{ terms}}$$
$$= \underbrace{\alpha(1) + \alpha(1) + \cdots + \alpha(1)}_{k \text{ terms}} = k\alpha(1).$$

So, we need only determine the choices for $\alpha(1)$ that make α an automorphism of Z_{10}. Since property 5 of Theorem 6.2 tells us that $|\alpha(1)| = 10$, there are four candidates for $\alpha(1)$:

$$\alpha(1) = 1, \qquad \alpha(1) = 3, \qquad \alpha(1) = 7, \qquad \alpha(1) = 9.$$

To distinguish among the four possibilities, we refine our notation by denoting the mapping that sends 1 to 1 by α_1, 1 to 3 by α_3, 1 to 7 by α_7, and 1 to 9 by α_9. So the only possibilities for Aut(Z_{10}) are α_1, α_3, α_7, and α_9. But are all these automorphisms? Clearly, α_1 is the identity. Let us check α_3. Since $x \bmod 10 = y \bmod 10$ implies $3x \bmod 10 = 3y \bmod 10$, α_3 is well defined. Moreover, because $\alpha_3(1) = 3$ is a generator of Z_{10}, it follows that α_3 is onto (and, by Exercise 12 in Chapter 5, it is also one-to-one). Finally, since $\alpha_3(a + b) = 3(a + b) = 3a + 3b = \alpha_3(a) + \alpha_3(b)$, we see that α_3 is operation-preserving as well. Thus, $\alpha_3 \in$ Aut(Z_{10}). The same argument shows that α_7 and α_9 are also automorphisms.

This gives us the elements of Aut(Z_{10}) but not the structure. For instance, what is $\alpha_3\alpha_3$? Well, $(\alpha_3\alpha_3)(1) = \alpha_3(3) = 3 \cdot 3 = 9 = \alpha_9(1)$, so $\alpha_3\alpha_3 = \alpha_9$. Similar calculations show that $\alpha_3^3 = \alpha_7$ and $\alpha_3^4 = \alpha_1$, so that $|\alpha_3| = 4$. Thus, Aut(Z_{10}) is cyclic. Actually, the following Cayley tables reveal that Aut(Z_{10}) is isomorphic to $U(10)$.

$U(10)$	**1**	**3**	**7**	**9**
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Aut(Z_{10})	α_1	α_3	α_7	α_9
α_1	α_1	α_3	α_7	α_9
α_3	α_3	α_9	α_1	α_7
α_7	α_7	α_1	α_9	α_3
α_9	α_9	α_7	α_3	α_1

∎

With Example 13 as a guide, we are now ready to tackle the group $\text{Aut}(Z_n)$. The result is particularly nice, since it relates the two kinds of groups we have most frequently encountered thus far—the cyclic groups Z_n and the U-groups $U(n)$.

■ Theorem 6.5 $\text{Aut}(Z_n) \approx U(n)$

For every positive integer n, $\text{Aut}(Z_n)$ is isomorphic to $U(n)$.

As in Example 13, any automorphism α is determined by the value of $\alpha(1)$, and $\alpha(1) \in U(n)$. Now consider the correspondence from $\text{Aut}(Z_n)$ to $U(n)$ given by T: $\alpha \to \alpha(1)$. The fact that $\alpha(k) = k\alpha(1)$ (see Example 13) implies that T is a one-to-one mapping. For if α and β belong to $\text{Aut}(Z_n)$ and $\alpha(1) = \beta(1)$, then $\alpha(k) = k\alpha(1) = k\beta(1) = \beta(k)$ for all k in Z_n, and therefore $\alpha = \beta$.

To prove that T is onto, let $r \in U(n)$ and consider the mapping α from Z_n to Z_n defined by $\alpha(s) = sr \pmod n$ for all s in Z_n. We leave it as an exercise to verify that α is an automorphism of Z_n (see Exercise 27). Then, since $T(\alpha) = \alpha(1) = r$, T is onto $U(n)$.

Finally, we establish the fact that T is operation-preserving. Let α, $\beta \in \text{Aut}(Z_n)$. We then have

$$\begin{aligned} T(\alpha\beta) &= (\alpha\beta)(1) = \alpha(\beta(1)) = \alpha(\underbrace{1 + 1 + \cdots + 1}_{\beta(1)}) \\ &= \underbrace{\alpha(1) + \alpha(1) + \cdots + \alpha(1)}_{\beta(1)} = \alpha(1)\beta(1) \\ &= T(\alpha)T(\beta). \end{aligned}$$

This completes the proof.

■ Theorem 9.4 $G/Z(G) \approx \text{Inn}(G)$

For any group G, $G/Z(G)$ is isomorphic to Inn(G).

Consider the correspondence from $G/Z(G)$ to $\text{Inn}(G)$ given by $T: gZ(G) \to \phi_g$ [where, recall, $\phi_g(x) = gxg^{-1}$ for all x in G]. First, we show that T is well defined. To do this, we assume that $gZ(G) = hZ(G)$ and verify that $\phi_g = \phi_h$. (This shows that the image of a coset of $Z(G)$ depends only on the coset itself and not on the element representing the coset.) From $gZ(G) = hZ(G)$, we have that $h^{-1}g$ belongs to $Z(G)$. Then, for all x in G, $h^{-1}gx = xh^{-1}g$. Thus, $gxg^{-1} = hxh^{-1}$ for all x in G, and, therefore, $\phi_g = \phi_h$. Reversing this argument shows that T is one-to-one, as well. Clearly, T is onto.

That T is operation-preserving follows directly from the fact that $\phi_g\phi_h = \phi_{gh}$ for all g and h in G.

EXERCISE 1

1. Show that the identity mapping on a group G is an automorphism.
2. Let G be the group of integers under addition. Show that the mapping $\phi : G \to G$ defined by $\phi(x) = -x, x \in G$ is an automorphism.
3. Let G be the group of complex numbers under addition. Show that the mapping $\phi : G \to G$ defined by $\phi(z) = \bar{z}, z \in G$ is an automorphism.
4. If G is a cyclic group of order 12, find the set of all automorphisms of the group G.
5. Let G be a finite group. Let f be an automorphism of G with the property : $f(x) = x$ for $x \in G$ if and only if $x = e$. Show that every $g \in G$ can be expressed as $(f(x))x^{-1}$ for some $x \in G$.
6. Let G be a finite group. Let f be an automorphism of G with the property : $f(x) = x$ for $x \in G$ if and only if $x = e$. If $f^2 = I$, then show that G is abelian.
7. In the group $\{1, -1, i, -i\}$ with respect to usual multiplication, show that inner automorphisms of the group corresponding to i and $-i$ are identical.
8. Let G be a group and ϕ an automorphism of G. If $a \in G$ is of finite order, then show that $o(\phi(a)) = o(a)$.
9. Let G be a finite cyclic group of order n. If the mapping $f : x \to x^m, x \in G$ is an automorphism, show that $(m, n) = 1$.
10. Show that the group of automorphism of a cyclic group is abelian.
11. Let G be an abelian group. Show that $H = \{x \in G : x^n = e, n$ being a fixed integer$\}$ is a characteristic group of G.
12. If G is a group, N a normal subgroup of G, H a characteristic subgroup of N, show that H is a normal subgroup of G.