Inner Automorphism →

An automorphism $I_g : G \to G$ defined by $I_g(x) = gxg^{-1}$, $x \in G$, is said to be an inner automorphism of G determined by g.

<u>REMARK</u>: It is also called the conjugation by g map.

☐ **Prove that the conjugation by g map is an automorphism.**

<u>Proof</u>: For $x, y \in G$, $I_g(xy) = g(xy)g^{-1} = gxg^{-1}gyg^{-1}$

$$= (gxg^{-1})(gyg^{-1})$$

$$= I_g(x) \circ I_g(y), \ \forall x, y \in G.$$

$\Rightarrow I_g$ is a homomorphism. ⟶ (i)

Let $I_g(x) = I_g(y) \Rightarrow gxg^{-1} = gyg^{-1} \Rightarrow g^{-1}(gxg^{-1}) = g^{-1}(gyg^{-1})$

$\Rightarrow xg^{-1} = yg^{-1} \Rightarrow x = y$.

$\Rightarrow I_g$ is injective. ⟶ (ii)

Let $I_g(x) = p \in G$. Then $gxg^{-1} = p$

$\Rightarrow xg^{-1} = g^{-1}p \Rightarrow x = g^{-1}pg \in G$.

∴ An arbitrary element $p \in G$ (codomain) has a pre-image $x (= g^{-1}pg)$ in G (domain).

$\Rightarrow I_g$ is surjective ⟶ (iii)

From (i), (ii) & (iii), it follows that I_g is an automorphism.

☐ **Show that $I_g = I_G$ if $g \in Z(G)$.**

If $g \in Z(G)$, then $gx = xg \ \forall x \in G$.

Now $I_g(x) = gxg^{-1} = xgg^{-1} = xe = x, \ \forall x \in G$.

$\Rightarrow$ <u>$I_g = I_G$</u>, the identity automorphism.

- $Inn(G) \to$ denotes the set of all inner automorphisms of G.
- $Inn(G) \leq Aut(G) \leq Perm(G)$.
- $Inn(G) \triangleleft Aut(G)$.

To Show: (i) $Inn(G) \leq Aut(G)$ (ii) $Inn(G) \triangleleft Aut(G)$.

(i) $I_e(x) = exe^{-1} = x$, $\forall x \in G$; $e \equiv$ identity of G.

$\Rightarrow I_e = I_G \in Inn(G)$.

$\Rightarrow Inn(G)$ is a non-empty subset of $Aut(G)$.

Let $I_{g_1}, I_{g_2} \in Inn(G)$. Then for $g_1, g_2 \in G$, we have

$$(I_{g_1} \circ I_{g_2})(x) = I_{g_1}(I_{g_2}(x)) = I_{g_1}(g_2 x g_2^{-1}) = g_1(g_2 x g_2^{-1})g_1^{-1}$$
$$= (g_1 g_2) x (g_1 g_2)^{-1} = I_{g_1 g_2}(x), \text{ where } g_1 g_2 \in G, \forall x \in G.$$

$\Rightarrow I_{g_1} \circ I_{g_2} \in Inn(G)$.

Now $(I_g \circ I_{g^{-1}})(x) = I_g(g^{-1}xg) = g(g^{-1}xg)g^{-1} = (gg^{-1})x(gg^{-1})$.
$= exe^{-1} = I_e(x)$, $\forall x \in G$.

Also, $(I_{g^{-1}} \circ I_g)(x) = I_{g^{-1}}(gxg^{-1}) = g^{-1}(gxg^{-1})g = exe^{-1} = I_e(x)$.

Hence $I_g \circ I_{g^{-1}} = I_{g^{-1}} \circ I_g = I_e$

$\Rightarrow I_{g^{-1}}$ is the inverse of I_g, and $I_{g^{-1}}(x) = g^{-1}x(g^{-1})^{-1} \in Inn(G)$. [Since $g^{-1} \in G$].

Hence,

$I_{g_1} \circ I_{g_2} \in Inn(G)$ and $I_{g^{-1}} \in Inn(G)$.

$\Rightarrow$ $\underline{Inn(G) \leq Aut(G)}$. (proved)

(ii) Let $\alpha \in Aut(G)$, and $I_g \in Inn(G)$.

$$(\alpha \circ I_g \circ \alpha^{-1})(x) = \alpha \circ [I_g\{\alpha^{-1}(x)\}] = \alpha \circ [g\alpha^{-1}(x)g^{-1}]$$
$$= \alpha(g)\{\alpha \circ \alpha^{-1}(x)\}\alpha(g^{-1}) \quad [\because \alpha \text{ is a homomor.}]$$
$$= \alpha(g) I_G(x) \alpha(g^{-1}) = \alpha(g)\, x\, [\alpha(g)]^{-1}$$
$$= I_{\alpha(g)}(x), \forall x \in G.$$

$\therefore \alpha \circ I_g \circ \alpha^{-1} \in Inn(G)$, for all $\alpha \in Aut(G)$.

$\therefore$ $\underline{Inn(G) \triangleleft Aut(G)}$. (proved)

Another Approach to

Show that $Inn(G) \leq Aut(G)$.

Proof: $I_e(x) = exe^{-1} = x, \forall x \in G$.

$\Rightarrow I_e = I_G \in Inn(G)$. $\Rightarrow Inn(G)$ is non-empty.

Let $I_{g_1}, I_{g_2} \in Inn(G)$, where $g_1, g_2 \in G$.

$$(I_{g_1} \circ I_{g_2})(x) = I_{g_1} \circ I_{g_2}(x) = I_{g_1}(g_2 x g_2^{-1})$$
$$= g_1(g_2 x g_2^{-1}) g_1^{-1} = (g_1 g_2) x (g_1 g_2)^{-1}$$
$$= I_{g_1 g_2}(x), \forall x \in G, [\because g_1 g_2 \in G]$$

$\Rightarrow I_{g_1} \circ I_{g_2} = I_{g_1 g_2} \in Inn(G)$.

Let $I_g \in Inn(G)$ for any $g \in G$.

I_g being a bijective map defined as $I_g : G \to G$ by $I_g(x) = gxg^{-1}, x \in G$, there exists a inverse map $I_g^{-1} : G \to G$ s.t.

Now let us assume $y \in G$ (codomain)

$y = I_g(x) = gxg^{-1}$ for $x \in G$ (domain).

$\Rightarrow x = g^{-1}yg \Rightarrow I_g^{-1}(y) = g^{-1}yg, y \in G$ (codomain)

i.e., we can write $\exists$ a inverse map I_g^{-1} of I_g s.t. $I_g^{-1}(x) = g^{-1}xg, x \in G$ (codomain).

$$= I_{g^{-1}}(x), x \in G.$$

$\therefore I_g^{-1} = I_{g^{-1}} \in Inn(G)$.

$\therefore$ $Inn(G) \leq Aut(G)$.

Theorem: G is an abelian group if and only if $I_g = I_G,\ \forall g \in G$.

Prove: Let G be abelian and $g \in G$.
Then $I_g(x) = gxg^{-1} = xgg^{-1} = xe = x,\ \forall x \in G$.
$\Rightarrow I_g = I_G,\ \forall g \in G$.

Conversely, let $I_g = I_G,\ \forall g \in G$
Then $I_g(x) = I_G(x),\ \forall x \in G$
$\Rightarrow gxg^{-1} = x,\ \forall x \in G, \forall g \in G$.
$\Rightarrow (gxg^{-1})g = xg \Rightarrow gx = xg,\ \forall x, g \in G$.
$\Rightarrow G$ is abelian.

□ **Cor:** If G be a non-abelian group, then G has a non-trivial inner automorphism.

Because, as G is non-abelian, $\exists$ distinct $a, b \in G$ s.t. $ab \neq ba$
$\Rightarrow a \neq bab^{-1} = I_b(a)$
$\therefore I_b(a) \neq a \Rightarrow I_b \neq I_G$.
$\Rightarrow$ Inner automorphism I_b is not equal to the trivial automorphism I_G.

Theorem: $Inn(G) \simeq G/Z(G)$. ⊛ Donot use this proof. An alternative is in pg. 12.

Proof: Let us consider the map $\phi : G \rightarrow Inn(G)$ by $\phi(x) = I_x\ \forall x \in G$.

We claim: ϕ is surjective. Because, if $I_x(g) = y \in G$, then $xgx^{-1} = y \Rightarrow g = x^{-1}yx \in G$
i.e., y has a pre-image $g = x^{-1}yx$ in G.

To show: ϕ is a homomorphism.
Let $x, y \in G$. Then $\phi(xy) = I_{xy} = I_x \circ I_y = \phi(x)\phi(y)$.
$\therefore \phi$ is an onto homomorphism.

[$\because I_{xy}$ is a homomorphism]

[$I_{xy}(g) = (xy)g(xy)^{-1}$
$= x(ygy^{-1})x^{-1} = I_x(ygy^{-1})$]

Determine $\ker\phi$:

$x \in \ker\phi \Leftrightarrow \phi(x) = I_e = I_G$ $\left[\because I_e(g) = ege^{-1} = g, \forall g \in G \Rightarrow I_e = I_G.\right]$

Remark: Alternative proof of this theorem is noted in page No. 12.

$\Leftrightarrow I_x = I_e$

$\Leftrightarrow I_x(g) = I_e(g), \ \forall g \in G.$

$\Leftrightarrow xgx^{-1} = ege^{-1} = g$

$\Leftrightarrow xg = gx, \ \forall g \in G.$

$\Leftrightarrow x \in Z(G).$

$\therefore \ker\phi = Z(G).$

$\therefore$ By the isomorphism theorem, we have

$$\underline{Inn(G) \simeq G/Z(G)}.$$

Theorem: Let G be a group and the map $\alpha : G \to G$ is defined by $\alpha(x) = x^{-1}$, $x \in G$. Then α is an automorphism if and only if G is abelian.

Proof: Let α be an automorphism and $x, y \in G$.

Then $\alpha(xy) = \alpha(x)\alpha(y) \Rightarrow (xy)^{-1} = x^{-1}y^{-1}$, $[\because \alpha$ is a homo...$]$

$\Rightarrow [(xy)^{-1}]^{-1} = (x^{-1}y^{-1})^{-1}$

$\Rightarrow xy = yx, \ \forall x, y \in G.$

$\Rightarrow$ $\underline{G \text{ is abelian}}$.

Conversely, let G be abelian.

Then for $x, y \in G$, $\alpha(xy) = (xy)^{-1} = y^{-1}x^{-1}$

$= x^{-1}y^{-1}$ $[\because G$ is abelian$]$

$= \alpha(x)\alpha(y).$

$\therefore \alpha$ is a homomorphism.

Let $\alpha(x) = \alpha(y) \Rightarrow x^{-1} = y^{-1} \Rightarrow (x^{-1})^{-1} = (y^{-1})^{-1} \Rightarrow x = y.$

$\therefore \alpha$ is injective.

Let $y \in G$ be arbitrary s.t. $\alpha(x) = y \Rightarrow x^{-1} = y$

$\Rightarrow (x^{-1})^{-1} = y^{-1} \Rightarrow x = y^{-1} \in G.$

$\therefore y$ has a pre-image $(x =) y^{-1}$ in G.

$\therefore \alpha$ is surjective, and therefore $\underline{\alpha \text{ is an automor...}}$

EXAMPLES OF AUTOMORPHISM : EX-15 (S.K. Mapa).

15. (i) Let $G = (\mathbb{C}, +)$ and $\phi : G \to G$ is defined by $\phi(z) = \bar{z}$, $z \in \mathbb{C}$. Show that ϕ is an automorphism.

Let $z_1, z_2 \in \mathbb{C}$. Then $\phi(z_1 z_2) = \overline{z_1 z_2} = \bar{z}_1 \bar{z}_2 = \phi(z_1)\phi(z_2)$

$\Rightarrow \phi$ is a homomorphism.

Let $\phi(z_1) = \phi(z_2) \Rightarrow \bar{z}_1 = \bar{z}_2 \Rightarrow \bar{\bar{z}}_1 = \bar{\bar{z}}_2 \Rightarrow z_1 = z_2$

$\Rightarrow \phi$ is one-one.

Let $p \in \mathbb{C}$ be arbitrary s.t. $\phi(z) = p$,

$\Rightarrow \bar{z} = p \Rightarrow \bar{\bar{z}} = \bar{p}$

$\Rightarrow z = \bar{p} \in \mathbb{C}$.

$\therefore p$ has a pre-image $(z=)\ \bar{p}$ in $\mathbb{C}$.

$\Rightarrow \phi$ is onto.

$\therefore \phi$ is a homomorphism and a bijection, hence ϕ is an automorphism.

(ii) Let $G = \{1, i, -1, -i\}$ and $\phi : G \to G$ is defined by $\phi(x) = x^3$, $x \in G$. Examine if ϕ is an automor...

Let $x, y \in G$. Then $\phi(xy) = (xy)^3 = x^3 y^3 = \phi(x)\phi(y)$

$\Rightarrow \phi$ is a homomorphism.

Let $\phi(x) = \phi(y) \Rightarrow x^3 = y^3 \Rightarrow x = y$ in G. [check!]

$\Rightarrow \phi$ is one-one.

ϕ is onto since each element of G has a pre-image in G.

$\therefore \phi$ is an automorphism.

(iii) Let $G = (\mathbb{Z}_6, +)$ and $\phi : G \to G$ is defined by $\phi(x) = 2\bar{x}$, $\bar{x} \in \mathbb{Z}_6$. Examine if ϕ is an auto...

Let $\bar{x}, \bar{y} \in \mathbb{Z}_6$. Then $\phi(xy) = 2\overline{xy} = 2\bar{x}\bar{y} \neq \phi(x)\phi(y)$

$\Rightarrow \phi$ is not a homomorphism.

$\therefore \phi$ is not an automorphism.

Check! ϕ is onto but not one-one. $\phi(\mathbb{Z}_6) = \{\bar{0}, \bar{2}, \bar{4}\}$ ← image set.

(iv) Let $G = (Z_5, +)$ and $\phi : G \to G$ is defined by $\phi(x) = 2\bar{x}$, $\bar{x} \in Z_5$.

Let $\bar{x}, \bar{y} \in Z_5$. Then $\phi(xy) = 2\overline{xy} = 2\bar{x}\bar{y} \neq \phi(x)\phi(y)$

$\Rightarrow \phi$ is not a homomorphism.

Image set $\phi(Z_5) = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\} = Z_5$.

ϕ is one-one and Z_5 is a finite set, so ϕ is onto also.

In any case, ϕ is not an automorphism

16. Let G be a commutative group of order n. If $\gcd(m, n) = 1$, prove that the mapping $\phi : G \to G$ defined by $\phi(x) = x^m$, $x \in G$ is an automorphism.

Let $a, b \in G$, and $\phi(a) = \phi(b)$

$$\Rightarrow a^m = b^m \Rightarrow a^m b^{-m} = e$$

$$\Rightarrow (ab^{-1})^m = e \quad [\because G \text{ is commutative}]$$

$$\Rightarrow o(ab^{-1}) \mid m$$

Since $o(G) = n$ and $ab^{-1} \in G$, then $o(ab^{-1}) \mid n$.

Since $\gcd(m, n) = 1$ and $o(ab^{-1}) \mid m$, $o(ab^{-1}) \mid n$, then $o(ab^{-1}) = 1 \Rightarrow ab^{-1} = e \Rightarrow a = b$.

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

$\therefore \phi$ is injective.

Since G is a finite group of order n and ϕ is injective $\Rightarrow \phi$ is surjective too.

$\therefore \phi$ is a bijection.

Now, $\phi(ab) = (ab)^m = a^m b^m \quad [\because G \text{ is commutative}]$

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

$\therefore \phi$ is an automorphism. (proved)