Automorphism Group of finite cyclic group

Example : $Aut(Z_{10})$

$Z_{10} = \{0,1,2,3,4,5,6,7,8,9\}, \oplus_{10}$

Z_{10} is finite cyclic group

its generators are $\langle 1\rangle, \langle 3\rangle, \langle 7\rangle, \langle 9\rangle$

Let $\alpha \in Aut(Z_{10})$

consider $\alpha(1)$

order of (1) is 10 (since $\langle 1\rangle$ of Z_{10})

$\Rightarrow \quad O(1) = 10$

and $\alpha \in Aut(Z_{10})$

i.e α is 1-1, onto, Homo , $\alpha : Z_{10} \to Z_{10}$

So, α preserves isomorphism

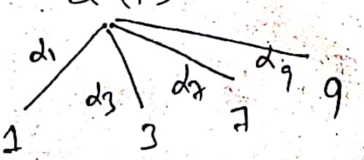
$\Rightarrow \quad |1| = |\alpha(1)|$ for $1 \in Z_{10}$

$\Rightarrow |\alpha(1)| = 10$

(property
$\phi : G \to G$ isomorphism
$\Rightarrow |a| = |\phi(a)|$
$\forall a \in G$)

In Z_{10}, $O(1) = 10$
$O(3) = 10$
$O(7) = 10$
$O(9) = 10$

$\therefore \quad \alpha(1)$



So, denoting the mapping that sends 1 to 1 by α_1
1 to 3 by α_3
1 to 7 by α_7
1 to 9 by α_9

So, only possibilities for $Aut(Z_{10})$ are $\alpha_1, \alpha_3, \alpha_7, \alpha_9$

Now check whether these are automorphism or not.

Scanned with CamScanner

Now α_1 maps 1 to 1

$\therefore \alpha_1(1) = 1$

$\Rightarrow \alpha_1(K) = K \cdot \alpha_1(1)$
$= K \cdot 1$
$= K$

[Now
$\alpha(1)$
$\alpha(2) = \alpha(1+1)$
$= \alpha(1) + \alpha(1)$ (α is Homo)
$= 2 \cdot \alpha(1)$
$\Rightarrow \alpha(K) = K\,\alpha(1)$]

$\Rightarrow \alpha_1$ is Identity map

$\therefore \alpha_1$ is Automorphism. ($\alpha_1 : Z_{10} \to Z_{10}$)

α_3 maps 1 to 3

to show: α_3 is 1-1, onto, Homo. ($\alpha_3 : Z_{10} \to Z_{10}$)

let $x = y$

$\Leftrightarrow x \bmod 10 = y \bmod 10$

$\Leftrightarrow 3x \bmod 10 = 3y \bmod 10$

$\Leftrightarrow 3x = 3y$

$\Leftrightarrow \alpha_3(x) = \alpha_3(y)$

1-1 & well defined

[$\alpha_3(x) = x \cdot \alpha_3(1)$]
$= x \cdot (3)$
$= 3x$

Also, α_3 is onto (using $f : S \to S$, S is finite & 1-1 $\Rightarrow f$ is onto)

$\therefore \alpha_3$ is 1-1, onto (Z_{10} is finite)

Now,

$\alpha_3(a+b) = (a+b)\,\alpha_3(1)$
$= 3(a+b)$
$= 3 \cdot a + 3b$
$= \alpha_3(a) + \alpha_3(b)$

$\therefore \alpha_3$ is Homo.

Hence $\alpha_3 \in Aut(Z_{10})$

Similarly $\alpha_7, \alpha_9 \in Aut(Z_{10})$

$\therefore Aut(Z_{10}) = \{\alpha_1, \alpha_3, \alpha_7, \alpha_9\}$

[Now, structure of $Aut(Z_{10})$ regarding operation
$\alpha_3 \alpha_7 = ?$
$\alpha_3 \alpha_3 = ?$]

Scanned with CamScanner

Now

$\alpha_3\alpha_3(1) = \alpha_3(\alpha_3(1))$

$= \alpha_3(3) \quad (\because \alpha_3(1) = 3)$

$= 3(\alpha_3(1))$

$= 3\cdot 3 = 9 = \alpha_9(1)$

$\alpha_3^2 = \alpha_3\alpha_3 = \alpha_9$

Now, $\alpha_3^3 = \alpha_3\alpha_3^2 = \alpha_3(9) = 3\cdot 9 = 27 = 7 \pmod{10}$
$= \alpha_7(1)$

$\alpha_3^4(1) = \alpha_3\alpha_3^3(1) = \alpha_3(7) = 7\cdot\alpha_3(1)$
$= 7\cdot 3 = 21 = 1$
$= \alpha_1(1)$

$\therefore \alpha_3^2 = \alpha_9$
$\alpha_3^3 = \alpha_7$
$\alpha_3^4 = \alpha_1$

$\therefore Aut(Z_{10}) = \langle \alpha_3 \rangle$

$\Rightarrow Aut(Z_{10})$ is cyclic

& $o(Aut(Z_{10})) = 4$

$\Rightarrow Aut(Z_{10}) \cong Z_4$ (cyclic grap of same order are isomorphic)

As $|U(10)| = 4$

$\therefore Aut(Z_{10}) \cong Z_4 \cong U(10)$ $(U(10) = \{1, 3, 7, 9\}, \otimes_{10})$

Cayles table

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

Remark: $\left\{\begin{array}{l} U(10) \text{ is cyclic} \\ \text{but } U(n) \text{ is need not be cyclic}, n \in \mathbb{N} \end{array}\right\}$

$Aut(Z_{10}) \cong U(10) \cong Z_4$ $(\because \phi(10) = 4)$

but $Aut(Z_n) \cong U(n) \not\cong Z_{\phi(n)}$ ($\because U(n)$ is need not be cyclic)

Scanned with CamScanner

Scanned with CamScanner

Automorphism Group of finite cyclic group

Theorem: For every positive Integer n, $Aut(Z_n) \cong U(n)$.

(proof) Let $G = \langle a \rangle$ where $a^n = e$ $(a \neq e)$ — (1)

with $o(G) = n$

Let $T \in Aut(G)$ be arbitrary

Since $T(a) \in G = \langle a \rangle$

$\Rightarrow T(a) = a^i$ for some $0 < i < n$ — (2)

(since $i = 0$

$\Rightarrow a^i = a^0 = e = T(a)$

$\Rightarrow a = T(a)$

$\Rightarrow a = e$ ($\because T$ is Automorphism so Identity map to Identity)

but by (1)

$a \neq e$

so, $i \neq 0$, Now take $i = n$ $\Rightarrow a^n = T(a)$

$\Rightarrow e = T(a)$

$\Rightarrow \Leftarrow$ again contradiction)

Since T is automorphism — (3)

$\Rightarrow o(T(a)) = o(a) = n$ (by property of automorphism)

claim: $\gcd(i, n) = 1$

Let, if possible

$\gcd(i, n) = k$; $k > 0$ is integer

(since in previous example $\alpha(1) \to 1, 3, 7, 9$ in Z_{10}

$$\left.\begin{matrix} \gcd(1, 10) \\ \gcd(3, 10) \\ \gcd(7, 10) \\ \gcd(9, 10) \end{matrix}\right] = 1$$)

$\Rightarrow k \mid i$ & $k \mid n$

$\Rightarrow \frac{i}{k}$ & $\frac{n}{k}$ both are positive integer

i.e $\frac{i}{k}, \frac{n}{k} \in Z^+$

Now, $(T(a))^{n/k} = (a^i)^{n/k}$

$= (a^n)^{i/k}$

$= e^{i/k} = e$

$\Rightarrow (T(a))^{n/k} = e$

Scanned with CamScanner

Since $o(T(a)) = n$

& $(T(a))^{n/k} = e$

$\Rightarrow$ n divides $\frac{n}{k}$ (by definition of order of element)

If $k \neq 1$

then $\frac{n}{k}$ is smaller than n

~~therefore~~ which is contradicts n divides $\frac{n}{k}$, if $k \neq 1$

$\therefore$ only possibility of $k = 1$

$\therefore$ $\gcd(i, n) = 1$

from ② & ③

we get structure of $Aut(G)$

$Aut(G) = \{T \mid T(a) = a^i, \text{ where } 0 < i < n, \gcd(i,n) = 1\}$

Now, for different value of i,

we get different Automorphism

provided $\gcd(i,n) = 1$, $0 < i < n$

which is same as definition of $\phi(n)$, Euler's phi function.

$\therefore$ $o(Aut(G)) = \phi(n)$

To show: $Aut(G) \cong U(n)$

Let $Aut(G) = \{T_i \mid T_i(a) = a^i, \langle a \rangle = G, 0 < i < n, \gcd(i,n) = 1\}$ [for different value of i we get different Auto.]

Define:

$\psi : U(n) \to Aut(G)$

defined as $\psi(i) = T_i \quad \forall\, i \in U(n)$

onto: Let $T_i \in Aut(G)$

then $\exists\, i \in U(n)$ s.t $\psi(i) = T_i$

$\Rightarrow$ ψ is onto map.

Scanned with CamScanner

Since $\psi(n)$ is finite
& $Aut(G)$ is finite & ψ is onto function
$\therefore$ ψ is 1-1 also

<u>Homomorphism</u>:

let $i, j \in \psi(n)$
then $\psi(ij) = T_{ij}$
let $a \in G = \langle a \rangle$

$$\Rightarrow T_{ij}(a) = a^{ij} = (a^j)^i = T_i(a^j) = T_i(T_j(a)) = T_i \circ T_j(a)$$

$$\Rightarrow T_{ij} = T_i \circ T_j = \psi(i) \circ \psi(j)$$

$$\Rightarrow \psi(ij) = \psi(i)\psi(j)$$

$\therefore$ ψ is Homomorphism

Hence $Aut(G) \cong U(n)$

Every finite cyclic group of order n is isomorphic to Z_n

$$\Rightarrow Aut(G) \cong Aut(Z_n) \cong U(n) \quad (\text{since } G \cong Z_n)$$

$$\Rightarrow Aut(Z_n) \cong U(n)$$

(Remark! another proof is given in Book also)

<u>Theorem</u> (9.4) $\dfrac{G}{Z(G)} \cong Inn(G)$, where G is group.

(proof) let define $T : \dfrac{G}{Z(G)} \to Inn(G)$

as $T(gZ(G)) = \phi_g$

where $Inn(G) = \{\phi_g \mid g \in G\}$

& $\phi_g(x) = gxg^{-1} \quad \forall x \in G$

Scanned with CamScanner

well-defined & 1-1

let $g\,Z(G) = h\,Z(G)$

$\Leftrightarrow h^{-1}g \in Z(G)$

$\Leftrightarrow h^{-1}gx = x h^{-1}g \quad \forall x \in G$ (by definition of $Z(G)$)

$\Leftrightarrow gxg^{-1} = hxh^{-1} \quad \forall x \in G$

$\Leftrightarrow \phi_g(x) = \phi_h(x) \quad \forall x \in G$

$\Leftrightarrow \phi_g = \phi_h$

$\Leftrightarrow T(g\,Z(G)) = T(h\,Z(G))$

Onto: let $\phi_g \in Inn(G)$

$\Rightarrow g \in G$

$\Rightarrow g\,Z(G) \in \frac{G}{Z(G)}$

such that $T(g\,Z(G)) = \phi_g$

$\Rightarrow T$ is onto

Homomorphism:

$T(g\,Z(G)\,h\,Z(G)) = T(gh\,Z(G))$ ($\because Z(G) \trianglelefteq G$)

$= \phi_{gh}$

$= \phi_g \phi_h$

$= T(g\,Z(G))\,T(h\,Z(G))$

$\therefore T$ is Homomorphism

Hence $\frac{G}{Z(G)} \cong Inn(G)$

(Question:) Find $Inn(D_6)$

D_6 is group of symmetry of regular hexagon

$O(D_6) = 6 \times 2 = 12$

By above theorem

$Inn(D_6) \cong \frac{D_6}{Z(D_6)}$

Scanned with CamScanner

$\therefore |D_6| = 2\times 6 = 12$

For $n \geq 3$, $Z(D_n) = \begin{cases} \{R_0, R_{180}\} & \text{if } n \text{ is even} \\ \{R_0\} & \text{if } n \text{ is odd} \end{cases}$

Here $n = 6$

$\therefore Z(D_6) = \{R_0, R_{180}\}$

$\Rightarrow o(Z(D_6)) = 2$

$|Inn(D_6)| = \dfrac{|D_6|}{|Z(D_6)|} = \dfrac{12}{2} = 6$

$\therefore o(Inn(D_6)) = 6 = 2\times 3$

{Result: If G is group of order $2p$, p is prime, $p \geq 3$ then $G \cong Z_{2p}$ or D_p }

$\therefore Inn(D_6) \cong Z_{2\times 3}$ or D_3

Now $Inn(D_6) \cong \dfrac{D_6}{Z(D_6)} \cong Z_6$ or D_3

If $\dfrac{D_6}{Z(D_6)} \cong Z_6 \Rightarrow \dfrac{D_6}{Z(D_6)}$ is cyclic ($\because Z_6$ is cyclic)

$\Rightarrow D_6$ is abelian (using result) If $\frac{G}{Z}$ is cyclic $\Rightarrow G$ is abelian)

But D_6 is Non-abelian

$\therefore Inn(D_6) \cong \dfrac{D_6}{Z(D_6)} \cong D_3$

Scanned with CamScanner