17. Let G be a group such that $Aut(G) = \{I_G\}$. Prove that G is a commutative group and $a^2 = e$ for all $a \in G$.

Let $a, b \in G$. Then $ab = I_G(ab)$
$= I_G(a) \circ I_G(b)$ [$\because I_G$ is an automorph.]
$= I_G(b) \circ I_G(a)$ [$\because Aut(G) = \{I_G\}$ is commutative]

Then $\Rightarrow \quad ab = ba$
$\Rightarrow$ G is commutative.

Now, $a^2 = a.a = I_G(a.a)$
$= I_G(a) \circ I_G(a)$ [$\because I_G$ is an automorph.]
$= I_G(a) \circ I_G^{-1}(a)$ [$\because I_G = I_G^{-1}$]
$= I_G(a) \circ I_G(a^{-1})$
$= I_G(a.a^{-1}) = I_G(e) = e$

$\therefore \quad a^2 = e \quad \forall a \in G.$ (proved)

Remark: Here G is commutative and all non-identity element have order 2.

Examples:

① Let G be a cyclic group of order 12. Examine if the map $\phi: G \to G$ defined by $\phi(x) = x^3$, $x \in G$, is an automorphism.

Let $G = \langle a \rangle$. Then $O(a) = 12$, as $O(G) = 12$.

Now $O(\phi(a)) = O(a^3) = \frac{O(a)}{gcd(3,12)} = \frac{12}{3} = 4.$

$\Rightarrow O(a) \neq O(\phi(a))$, showing that ϕ does not preserve the order of elements. So ϕ is not an isomorphism.

$\therefore$ ϕ is NOT an automorph.

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

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

$\Rightarrow (ab^{-1})^m = e$ [$\because G$ 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, $\phi(ab) = (ab)^m = a^m b^m$ [$\because G$ is commutative]

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

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

(2) Let $G = S_3$. Examine if the map $\phi : G \to G$ defined by $\phi(x) = x^{-1}$, $x \in G$, is an automorph..

As S_3 is a non-abelian group, the map $\phi(x) = x^{-1}$ fails to be homomorphism.

$\therefore$ $\phi : S_3 \to S_3$ defined by $\phi(x) = x^{-1}$ cannot be an automorphism.

(3) Let $G = \langle a \rangle$ and $O(G) = n$. Prove that $Aut(G)$ is a group of order $\phi(n)$, where $\phi(n)$ is the number of positive integers less than n and prime to n. [That is to prove: If $G = \langle a \rangle$ and $O(G) = n$, then $O(Aut(G)) = \phi(n)$]

Let $T : G \to G$ be an automorphism, $\in Aut(G)$.

since a is a generator of G,

so $\phi(a)$ " " " " $\phi(G) = G$ here.

Now the generators of G are a^m, where $m < n$ and $\gcd(m, n) = 1$.

Let us take m s.t. $m < n$ and $\gcd(m, n) = 1$ and consider the map $T : G \to G$ defined by $T(x) = x^m$, $x \in G$.

T is a homomorphism, because for $x, y \in G$, $T(xy) = (xy)^m = x^m y^m$ [$\because G$ is abelian]

$= T(x) T(y)$.

$\ker T = \{x \in G : T(x) = e_G\}$

Now $x \in G \Rightarrow O(x) \mid n$; $T(x) = e_G \Rightarrow x^m = e_G$

$\Rightarrow O(x) \mid m$.

Since $\gcd(m, n) = 1$, $O(x) \mid m$, $O(x) \mid n$, $\Rightarrow O(x) = 1$.

$\Rightarrow x = e_G \Rightarrow \ker \phi = \{e_G\} \Rightarrow T$ is one-to-one.

Since G is finite, T is onto also.

$\therefore$ T becomes an automorphism.

$\therefore$ The number of automorph... of $G = \phi(n)$. (proved)

Ex. Determine the elements of $Aut(Z_{10})$.

Z_{10} forms a group w.r.t. addition mod 10, $\oplus_{10}$.

$(Z_{10}, \oplus_{10}) = \langle \bar{1} \rangle$. Other generators are: $\bar{3}, \bar{7}, \& \bar{9}$ [integer < 10 & prime to 10].

Any automorphism of the group $(Z_{10}, \oplus_{10})$ will completely depend on where $\bar{1}$ is sent by the automorphism:

$\phi_{\bar{1}}$: $\bar{1} \to \bar{1}$, $\bar{2} \to \bar{2}$, ..., $\bar{9} \to \bar{9}$ } identity automorph.

$\phi_{\bar{3}}$: $\bar{1} \to \bar{3}$, $\bar{2} \to \bar{6}$, $\bar{3} \to \bar{9}$, $\bar{4} \to \bar{2}$, $\bar{5} \to \bar{5}$, $\bar{6} \to \bar{8}$, $\bar{7} \to \bar{1}$, $\bar{8} \to \bar{4}$, $\bar{9} \to \bar{7}$, $\bar{0} \to \bar{0}$ } [because, generator has to go to generator]

Similarly,

$\phi_{\bar{7}} : \bar{1} \to \bar{7}$, $\phi_{\bar{9}} : \bar{1} \to \bar{9}$

$\therefore$ The only possible automorphisms in the group $(Z_n, \oplus_{10})$ are $\phi_{\bar{1}}, \phi_{\bar{3}}, \phi_{\bar{7}}, \phi_{\bar{9}}$

$\therefore Aut(Z_n) = \{\phi_{\bar{1}}, \phi_{\bar{3}}, \phi_{\bar{7}}, \phi_{\bar{9}}\}$.

Infact, the formula for finding the automorphism for the group $(Z_n, \oplus_{10})$ is as follows:

$\phi_{\bar{1}}(\bar{K}) = \bar{K}$, $\bar{K} \in Z_n$

$\phi_{\bar{3}}(\bar{K}) = \bar{3}K$

$\phi_{\bar{7}}(\bar{K}) = \bar{7}.K$

$\phi_{\bar{9}}(\bar{K}) = \bar{9}.K$

Because, as for example,

$\phi_{\bar{3}}(\bar{1}) = \bar{3}$, $\phi_{\bar{3}}(\bar{2}) = \phi_{\bar{3}}(\bar{1}) + \phi_{\bar{3}}(\bar{1})$

$= \bar{3} + \bar{3}$

$= 2.\bar{3}$

$\phi_{\bar{3}}(\bar{3}) = \bar{3} + \bar{3} + \bar{3}$

$= 3.\bar{3}$

$\phi_{\bar{3}}(\bar{K}) = \bar{3} + \ldots + \bar{3}$ (K times)

$= K.\bar{3}$