Proof: Let ~~us~~ us consider the mapping $\phi : G \to Inn(G)$ by $\phi(x) = I_x$. Then ϕ is clearly surjective.

To show that ϕ is a homomorphism, let $x, y \in G$.

Then $\phi(xy) = I_{xy} = I_x \circ I_y = \phi(x) \circ \phi(y)$. So, ϕ is a homomorphism.

Let us determine $Ker\, \phi$.

$x \in Ker\, \phi \Leftrightarrow \phi(x) = I_e \Leftrightarrow (\phi(x))(g) = I_e(g)$ for all $g \in G$,

$\Leftrightarrow xgx^{-1} = g$ for all $g \in G$.

$\Leftrightarrow xg = gx$ for all $g \in G$

$\Leftrightarrow x \in Z(G)$. Hence $Ker\, \phi = Z(G)$

So, by first isomorphism theorem, $Inn(G)$ is isomorphic to the quotient group $G/Z(G)$, i.e., $Inn(G) \simeq G/Z(G)$

Note 1.1.11. Let $\phi : G \to G$ be an isomorphism, where G is a group. Then $o(a) = o(\phi(a))$ for $a \in G$.

Proof: Case 1 Let $o(a)$ be infinite. If possible, let $o(\phi(a)) = k$, k is a positive integer, then $(\phi(a))^k = e$, e is the identity in G.

So, $\phi(a^k) = e$ (As ϕ is an isomorphism)

$= \phi(e)$

So, $a^k = e$ (As ϕ is injective mapping)

So, $o(a)$ is finite, a contradiction. So, $o(\phi(a))$ is infinite

Case 2 Let $o(a)$ be finite and $o(a) = n$, n is a positive integer.

~~Let $o(\phi(a)) = k$~~ Then $(\phi(a))^n = \phi(a^n)$ (As ϕ is an isomorphism)

$= \phi(e)$ [As $a^n = e$]

$= e$ [As $\phi(e) = e$]

So, $o(\phi(a))$ is finite. Let $o(\phi(a)) = k$

So, k divides n. Now $\phi(a^k) = (\phi(a))^k = e$ [As $o(\phi(a)) = k$]

$= \phi(e)$

As ϕ is injective, so, $a^k = e$, So, ~~of~~ n divides k

Hence $k = n$ So, $o(\phi(a)) = n$

Theorem 1.1.12 If G be an infinite cyclic group then $Aut(G)$ is a group of order 2.

Proof: Since G is an infinite cyclic group, G is isomorphic to $(\mathbb{Z}, +)$. So, it is sufficient to determine all automorphism of $(\mathbb{Z}, +)$. Let ϕ be an automorphism of $(\mathbb{Z}, +)$. Since 1 is a generator the cyclic group $(\mathbb{Z}, +)$, $\phi(1)$ is also a generator of the ~~cyclic group~~ image group $(\mathbb{Z}, +)$. Since the only generators of the group $(\mathbb{Z}, +)$ are 1 and -1, so, $\phi(1) = 1$ or -1

If $\phi(1) = 1$, then $\phi(n) = n$ for each $n \in \mathbb{Z}$. In this case ϕ is the identity automorphism.

If $\phi(1) = -1$, then $\phi(n) = -n$ for each $n \in \mathbb{Z}$

So, there are only two automorphisms of G, i.e., $o(Aut(G)) = 2$

Note 1.1.13 The Theorem 1.1.12 can be written as follows: Let G be ~~a group~~ an infinite cyclic group. Then G has just one non-trivial automorphism.

Theorem 1.1.13 Let $G = \langle a \rangle$ be a finite cyclic group of order n. Then the mapping $\theta : G \to G$, defined by $\theta(a) = a^m$ is an automorphism of G if and only if m is relatively prime to n and less than n. In particular, G has $\phi(n)$ automorphism where $\phi(n)$ is the number of positive integers less than n and prime to n.

Proof: Let $G = \langle a \rangle$ be a cyclic group of order n and let $\theta : G \to G$ be an automorphism. Since a is a generator of G and θ is an automorphism, $\theta(a)$ is a generator of G. The generators of G are a^m, where m is less than n and prime to n.

So, $\theta(a) = a^m$ for some m which is less than n and relatively prime to n. Moreover θ is completely determined by its value on a as for any element $a^k \in G$, $\phi(a^k) = (\phi(a))^k = a^{km}$.

Conversely, given any positive integer m less than n and relatively prime to n, the mapping $\psi: G \to G$ defined by $\psi(a) = a^m$ can be extended to an automorphism of G, by defining $\psi(a^k) = a^{mk}$, $a^k \in G$. Then $\psi(a^i a^j) = \psi(a^{i+j}) = a^{m(i+j)}$ $= a^{mi} \cdot a^{mj} = \psi(a^i)\psi(a^j)$. Moreover ψ is injective because if $\psi(a^i) = \psi(a^j)$ then $a^{mi} = a^{mj}$ or, $a^{m(i-j)} = e$, e is the identity element in G. Since $o(a) = n$, n divides $m(i-j)$ and since n is relatively prime to m, n divides $i-j$. Hence $a^{i-j} = e$ or $a^i = a^j$ showing that ψ is injective.

Also ψ is surjective, for, let $b \in G$, so, $b = a^i$, $0 \le i \le n-1$. Since m is less than n and relatively prime to n, there exist integers k and l such that $km + ln = 1$. Hence we have $b = a^i = a^{i(km+ln)} = a^{mki} = \psi(a^{ki})$. Hence ψ is an automorphism. So, $o(Aut(G)) = \phi(n)$.

<u>Corollary 1.1.14</u> Any cyclic group G of order $n > 2$ has an automorphism which is not an inner automorphism.

Proof: As G is cyclic, G is abelian. Since G is abelian, any inner automorphism of G is trivial. Since G has $\phi(n)$ automorphism and $\phi(n) > 1$ when $n > 2$, G has an automorphism which is not an inner automorphism.

Worked Examples 1.1.15 :

1. Find the number of inner automorphisms of the group S_3.

Solution: Let $Z(S_3)$ be the centre of the group S_3. Since S_3 is a non-commutative group, $Z(S_3)$ is a proper subgroup of S_3. The quotient group $S_3/Z(S_3)$ is a non-cyclic group (we have used the following theorem: If G be a non-commutative group with centre $Z(G)$ then the quotient group $G/Z(G)$ is non-cyclic (S.K. Mapa, Theorem 2.15.4, Page-143)). Since S_3 is a finite group of order 6, the order of the group $Z(S_3)$ is a divisor of 6. Clearly, $o(Z(S_3)) \neq 6$. If $o(Z(S_3))=2$ then the order of the quotient group $S_3/Z(S_3)$ is 3, an ~~impossible~~ impossibility (As the group would be cyclic). If $o(Z(S_3))=3$, then the order of $S_3/Z(S_3)$ is 2, an impossibility in a similar fashion.

So, $o(Z(S_3))=1$. Consequently, the quotient group $S_3/Z(S_3)$ is ~~isom~~ isomorphic to the group S_3. Since the group $Inn(S_3)$ is isomorphic to the quotient group $S_3/Z(S_3)$, it follows that $Inn(S_3)$ is isomorphic to S_3. So $Inn(S_3)$ is a group of order 6. Hence the number of inner automorphism of the group S_3 is 6.

2. Show that $Aut(S_3)$ is also isomorphic to S_3.

Solution: In problem 1, we have seen that $Inn(S_3) \simeq S_3$. In our group theory, we have seen that $S_3 = \{e, a, a^2, b, ab, a^2b\}$ (where e is the identity permutation) with the defining relation $a^3 = e = b^2$, $ba = a^2b$.

The elements a and a^2 are of order 3 and b, ab and a^2b are all of order 2. Hence for any $\sigma \in Aut(S_3)$,