Thm:- for every positive integer n, $Aut(Z_n)$ is isomorphic to $U(n)$.

Proof:- Consider the correspondence from $Aut(Z_n)$ to $U(n)$ given by $T: \alpha \to \alpha(1)$.

Then we show that T is an isomorphism.

one-one:- Let $T(\alpha) = T(\beta)$

$\Rightarrow \alpha(1) = \beta(1)$

$\Rightarrow k\alpha(1) = k\beta(1)$

$\Rightarrow \alpha(k) = \beta(k) \quad \forall\ k \text{ in } Z_n$

$\Rightarrow \alpha = \beta$.

$\Rightarrow T$ is one-one.

onto: Let $r \in U(n)$.

Then consider the mapping $\phi: Z_n \to Z_n$ as

$\phi(s) = sr \pmod n$ for all s in Z_n.

Then we show that ϕ is an automorphism of Z_n.

ϕ is 1-1: Let $\phi(s_1) = \phi(s_2)$

$\Rightarrow s_1 r \pmod n = s_2 r \pmod n$

$\Rightarrow s_1 r r^{-1} \pmod n = s_2 r r^{-1} \pmod n$

($\because r^{-1}$ exists in Z_n)

$\Rightarrow s_1 \pmod n = s_2 \pmod n$

$\Rightarrow s_1 = s_2$.

ϕ is onto. Let $x \in Z_n$, then $\exists\ s \in Z_n$ s.t.

$$sr \pmod n = x$$

$$\Rightarrow \quad \phi(s) = x.$$

$\Rightarrow$ ϕ is onto.

ϕ preserves operation.

$$\phi(x+y) = (x+y)r \pmod n$$

$$= xr \pmod n + yr \pmod n$$

$$= \phi(x) + \phi(y)$$

$\Rightarrow$ ϕ is automorphism of Z_n

$\therefore$ for every $r \in U(n)$, $\exists$ a $\phi \in Aut(Z_n)$ such that $T(\phi) := \phi(1) = r$.

$\Rightarrow$ T is onto.

T preserves operation.

Let $\alpha, \beta \in Aut(Z_n)$, Then

$$T(\alpha\beta) = (\alpha\beta)(1) = \alpha(\beta(1))$$

$$= \alpha(\underbrace{1+1+\cdots+1}_{\beta(1) \text{ times}})$$

$$= \alpha(1) + \alpha(1) + \cdots + \alpha(1)$$

$$= \alpha(1)\,\beta(1)$$

$$= T(\alpha)\,T(\beta)$$

$\Rightarrow$ T preserves operation

$\Rightarrow$ T is an homomorphism Hence $Aut(Z_n) \cong U(n)$

Recap!-

Normal subgroups!- A subgp H of a group G is called a normal subgp of G if $aH = Ha \quad \forall a \in G$

N.S. Pert!- A subgp H of G is normal in G iff $xHx^{-1} \subseteq H \quad \forall x \in G$.

Ex!- (i) Every subgp of an abelian gp is normal
(ii) The center $Z(G)$ of a gp is always normal

Factor groups!- Let G be a gp and H a normal subgp of G. The set $G/H = \{aH \mid a \in G\}$ is a gp under operation $(aH)(bH) = (ab)H$.

Ex: $4\mathbb{Z} = \{0, \pm 4, \pm 8, \ldots\}$.

$$\frac{\mathbb{Z}}{4\mathbb{Z}} = \{0+4\mathbb{Z}, 1+4\mathbb{Z}, 2+4\mathbb{Z}, 3+4\mathbb{Z}\}$$

$0+4\mathbb{Z} = \{0, \pm 4, \pm 8, \ldots\}$

$1+4\mathbb{Z} = \{1, 5, 9, \ldots; -3, \ldots\}$

$2+4\mathbb{Z} = \{2, 6, 10, \ldots; -2, -6, -10, \ldots\}$

$3+4\mathbb{Z} = \{3, 7, 11, \ldots; -1, -5, -9, \ldots\}$.

Thm!- $G/Z(G) \cong Inn(G)$.

For any gp G, $G/Z(G)$ is homomphic to $U(n)$

Proof!- Consider the correspondence $T: G/Z(G) \to U(n)$ as $T(gZ(G)) = \phi_g \quad (\phi_g(x) = gxg^{-1})$

T is well-defined. Let $gZ(G) = hZ(G)$

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

Then for any $x \in G$ $h^{-1}gx = xh^{-1}g$

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

$\Rightarrow \phi_g = \phi_h$.

one-one Let $T(gZ(G)) = T(hZ(G))$

$\Rightarrow \phi_g = \phi_h$

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

$\Rightarrow h^{-1}gx = xh^{-1}g \quad \forall x \in G$

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

$\Rightarrow gZ(G) = hZ(G)$.

onto, for any $\phi_g \in Inn(G)$, then

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

Operation pres:- $T((gZ(G))(hZ(G))) = T((gh)Z(G))$

$= \phi_{gh}$

$= \phi_g \phi_h$

$= T(gZ(G))\, T(hZ(G))$

$\Rightarrow$ T preserves operation.

$\therefore$ T is an isomorphism.

$\Rightarrow Inn(G) \cong G/Z(G)$.

Ex:- $Inn(D_4) = \{\phi_{R_0}, \phi_{R_{90}}, \phi_H, \phi_D\}$.

$Z(D_4) = \{R_0, R_{180}\}$.

$D_4/Z(D_4) = \{Z(D_4), R_{90}Z(D_4), HZ(D_4), DZ(D_4)\}$.

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

Characteristic Subgp:- A subgp N of a gp G is called a characteristic subp if $\phi(N) = N$ for every $\phi \in Aut(G)$.

Ex:- Take Z_6

$Aut(Z_6) = \{\alpha_1, \alpha_5\}$ $\quad Aut(Z_6) \cong U(6)$ $\quad \{1, 5\}$

$N = \langle 2 \rangle = \{0, 2, 4\}$

then $\alpha_1(N) = N$

$\alpha_5(0) = 0 \quad \alpha_5(2) = 4 \quad \alpha_5(4) = 2$.

$\alpha_5(N) = N$.

$\Rightarrow \langle 2 \rangle$ is a characteristic subgp of Z_6.

Thm:- Every subgp of a cyclic gp is characteristic

Proof:- Let G be the cyclic gp, then if G is infinite, then G is isomorphic to Z.

Let $\phi: Z \to G$ be the isomorphism.

Let H be a subgp of G.

then $H = \langle \phi(k) \rangle$ for some k.

and $\alpha \in Aut(G)$

$\alpha(H) = H$.

Now, let G is finite. Then G is isomorphic to Z_n if $|G| = n$.

Let H be the subgp of Z_n. then

$H = \langle a^{n/k} \rangle$ for some k divisor of n.

Let ϕ be an automorphism of Z_n.

then $\phi : Z_n \to Z_n$

and $\phi(H)$ is a subgp of Z_n

and $|\phi(H)| = k$.

also $|H| = k$

$\Rightarrow \phi(H) = H$ (∵ fundamental theorem of cyclic Groups)

↓

fundamental theorem of Cyclic gps :-

Every subgp of a cyclic gp is cyclic. Moreover, if $|\langle a \rangle| = n$, then the order of any subgp of $\langle a \rangle$ is a divisor of n; and, for each positive divisor k of n, the gp $\langle a \rangle$ has exactly one subgp of order k - namely $\langle a^{n/k} \rangle$.

Thm:- Center of a gp is characteristic.

Proof:- Let G be a gp and $Z(G)$ is the center of G

Let $\phi : G \to G$ be a automorphism

then for every $x \in Z(G)$, $\phi(x) \in Z(G)$

$\left(\because xg = gx \Rightarrow \phi(x)\phi(y) = \phi(y)\phi(x) \right.$

$\left. \forall\, g \in G \Rightarrow \phi(g) \in G \right)$

Therefore. $\phi(Z(G)) = Z(G)$

$\Rightarrow Z(G)$ is characteristic.

Thm:- The characteristic property is transitive i.e. Let N is a characteristic subgp of K and K is a characteristic subgp of G, then N is characteristic subgp of G.

Pwf Let $\phi : G \to G$ be automorphism.

then $\phi(K) = K$ ($\because K$ is characteristic of G)

$\therefore \phi|_K : K \to K$ is automorphism

$\Rightarrow \phi_{|K}(N) = N$ ($\because N$ is characteristic of K)

Hence $\phi(N) = N$

This is true for all $\phi \in Aut(G)$.

$\Rightarrow$ N is characteristic subgp of G.