Group Theory
Assignment - 1.

TRISHAN MONDAL.
Bmat - 2144

① G be a group. It's given that $Aut(G) = \{\tilde{e}\}$. ($\tilde{e} \to$ identity map)
We know, $Inn(G) \leq Aut(G)$. So, $Inn(G) = \{\tilde{e}\}$.
Also, $Z(G)$ be the Center of G. We know

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

$$\text{So, } G/Z(G) \cong \{\tilde{e}\}.$$

So, $G = Z(G)$ Since, $Z(G)$ is normal Subgroup of G.
So, every element of $G = Z(G)$ Commutes will all other elements.

$$\therefore G \text{ is abelian.}$$

- Assume, G is finite. $Aut(G) = \{e\}$. Then $\forall x \in G$ ~~x Should be mapped~~ $x \mapsto x^{-1}$ is an Auto morphism as G is abelian.

But, $Aut(G) = \{e\}$ So, $x^{-1} = x$ $\forall x \in G$.

$$\Rightarrow \boxed{x^2 = e}. \quad \forall x \in G$$

So, Either $G = \{e\}$ or, $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}$.
$\cong (\mathbb{Z}/2\mathbb{Z})^n$.

Consider $n > 1$. (We will work, taking $G = (\mathbb{Z}/2\mathbb{Z})^n$)**
Define, $\varphi: G \to G$ as following,

$$\varphi(x_1, \dots, x_n) = (x_n, x_2, \dots, x_1) \text{ [Swap 1st and nth Co-ordinate]}$$

- φ is well defined.
Let, $g \in G$ and $g' \in G$ s.t

$$g = g' = (\tilde{x}_1, \dots, \tilde{x}_n)$$
$$\therefore \varphi(g) = (\tilde{x}_n, \dots, \tilde{x}_1)$$
$$\varphi(g') = (\tilde{x}_n, \dots, \tilde{x}_1)$$
$$\therefore \varphi(g) = \varphi(g').$$

• φ is an Automorphism.

Let, $g_1 = (x_1, --, x_n)$
$g_2 = (y_1, --, y_n)$

$$\varphi(g_1 g_2) = \varphi(x_1+y_1, --, x_n+y_n)$$
$$= (x_n+y_n, --, x_1+y_1)$$
$$= (x_n, --, x_1) \cdot (y_n, --, y_1)$$
$$= \varphi(g_1)\varphi(g_2).$$

So, φ is Homo-morphism.

• φ is clearly injective.

Now, $\forall (\tilde{x}_1, --, \tilde{x}_n)$ tuple $\in G$, we get,
$$(\tilde{x}_n, \tilde{x}_2, --, \tilde{x}_1) \in G \text{ s.t.}$$
$$\varphi(\tilde{x}_n, --, \tilde{x}_1) = (\tilde{x}_1, --, \tilde{x}_n).$$

$\Rightarrow \varphi$ is surjective.

$\therefore \varphi$ is an Automorphism.

Clearly, for $n>1$ $(x_1, --, x_n) \neq (x_n, --, x_1)$ $\forall (x_1, --, x_n) \in G = (\mathbb{Z}/2\mathbb{Z})^n$

So, φ is non-trivial Auto-morphism.

So, for $n>1$, $G = (\mathbb{Z}/2\mathbb{Z})^n$ has a non-trivial Automorphism

So, $\mathrm{Aut}(G) \neq \{\tilde{e}\}$.

Hence, $n=1$ only case for which $G = \mathbb{Z}/2\mathbb{Z}$ is staisfying the given property.

$\therefore |G| = 2$.

So, $O(G)$ is either 1 or 2. ■

** <u>Rem</u>: Everything will follow from Isomorphism.

② Consider, Ω be the infinite set but Countable.

Take $G_1 = (\mathbb{Z}/4\mathbb{Z})^{\Omega}$.

$G_2 = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})^{\Omega}$.

- Consider, $\varphi : G_1 \to G_2$ by.

$$\varphi(g_1, g_2, \dots) = (0, g_1, g_2, \dots)$$

This is clearly injective group Homomorphism.
So, $\exists H_2 \leqslant G_2$ Such that, $G_1 \cong H_2$.

- Consider, $\tilde{\varphi} : G_2 \to G_1$ by,

$$\tilde{\varphi}(g_1, g_2, \dots) = (2g_1, g_2, \dots)$$

$\forall a, b \in \mathbb{Z}/2\mathbb{Z}$, $a - b \equiv 0 \pmod 2$

$2a - 2b \equiv 0 \pmod 4$.

So, $\forall g_1 \in \mathbb{Z}/2\mathbb{Z}$, $2g_1$ is unique element in $\mathbb{Z}/4\mathbb{Z}$.
So, $\tilde{\varphi}$ is well defined. It's easy to see,

$$\tilde{\varphi}((g_1, g_2, \dots) + (\tilde{g}_1, \tilde{g}_2, \dots)) = (2\tilde{g}_1 + 2g_1, g_2 + \tilde{g}_2, \dots)$$
$$= \tilde{\varphi}(g_1, g_2, \dots)\,\varphi(\tilde{g}_1, \tilde{g}_2, \dots)$$

Now, Notice that first Co-ordinate maps from $\mathbb{Z}/2\mathbb{Z}$ to unique element of $\mathbb{Z}/4\mathbb{Z}$ and other elements (Co-ordinate) will map to it self.

So, $\tilde{\varphi}$ is injective.

So, $\exists H_1 \leqslant G_1$ s.t $H_1 \cong G_2$.

- Suppose, there exist an isomorphism from G_1 to G_2.

Say, $\phi : G_1 \to G_2$ be that isomorphism.

Let, $a \in G_1$ Such that $\phi(a) = (1, 0, \dots) \in G_2$

isomorphism preserves order So, $\mathrm{Ord}_{G_1}(a) = 2$.

So, all Co-ordinates of a will be either 0 or 2.

Take, $a = (a_1, \dots)$, $b = \left(\frac{a_1}{2}, \frac{a_2}{2}, \dots\right)$

$\phi(b)$ must have 1, or 0 in first Co-ordinate.

if, $\phi(b) = (0, g_1, \cdots)$ then,

$\phi(a) = \phi(b) + \phi(b) = (0, 2g_1, \cdots)$

Contradicts that $\phi(a) = (4, 0, \cdots)$.

if $\phi(b) = (1, g_1, \cdots)$ then,

$\phi(a) = \phi(b) + \phi(b) = (0, 2g_1, \cdots)$

Again Contra-diction!

So, G_1 and G_2 are not isomorphic. ■

If, $|G_1|, |G_2| < \infty$ then,

$G_2 \simeq H \subseteq G_1 \Rightarrow |G_2| \leq |G_1|$

$G_1 \simeq G \subseteq G_2 \Rightarrow |G_1| \leq |G_2|$

$\Rightarrow |G_1| = |G_2|$.

So, Clearly there is isomorphisom b/w G_1 and G_2 ■

(by taking $H = G_1$).

③ R is a Commutative Ring. With identity 1. i.e R is abalian w.r.t multiplication.

$$U = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \middle| x \in R \right\}.$$

take, $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \in U$. Now,

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix}$$ (As 1 is identity of multiplication on R)

Since, R is Ring $x+y \in R$ $\forall x, y \in R$.

$\therefore$ $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \in U$.

Since, R is Ring $\forall x \in R$, $(-x)$ (inverse ~~wr~~ of x w.r.t addition) $\in R$.

$$\therefore \begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix} = I_2$$

We know I_2 = identity element of $SL_2(R)$. So, I_2 has to be identity of U under operation "Matrix Multiplication".

So, $\forall A \in U$, A^{-1} is ~~d~~ exsits and Canbe determined uniquely.

So, U is a "Group".

- We Can notice that "U" is Abelian.

Define, $\varphi : (R, +) \longmapsto U$ as,

$$\varphi(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

(*)

So, $\varphi(x+y) = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \varphi(x)\varphi(y)$.

So, φ is Homomorphism.

(*) Take, $x = \tilde{x} \in (R, +)$

$\Rightarrow \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \tilde{x} \\ 0 & 1 \end{pmatrix}$

$\Rightarrow \varphi(x) = \varphi(\tilde{x})$

So, φ is well defined.

We can see that $\forall\ x \in (R, +)$. we can get

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in U.$$

~~As~~ Also, $\forall x \in R$, $x \in (R, +)$ [because, R is ring and Ring is def: a group on $(+, \cdot)$]

$\therefore \forall x \in R$ or $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in U$ we can see

$$\varphi(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}.$$

So, φ is both injective and surjective

$\therefore \varphi$ is isomorphism.

$$\therefore \boxed{(R, +) \cong U.}$$

■

4. We know $SL_3(\mathbb{F}_3) = \left\{ A \mid \begin{array}{l} A \to \text{order 3 square Matrix} \\ \text{elements of } A \text{ belong to } \mathbb{F}_{P(=3)} \\ \det(A) = 1 \end{array} \right\}$

Now, $U(3, \mathbb{F}_3) = \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \middle| \; x, y, z \in \mathbb{F}_3 \right\} \subset SL_3(\mathbb{F}_3)$.

Take, $\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & \tilde{x} & \tilde{y} \\ 0 & 1 & \tilde{z} \\ 0 & 0 & 1 \end{pmatrix} \in U(3, \mathbb{F}_3)$.

(existance of product) $\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \tilde{x} & \tilde{y} \\ 0 & 1 & \tilde{z} \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+\tilde{x} & y+\tilde{y}+x\tilde{z} \\ 0 & 1 & z+\tilde{z} \\ 0 & 0 & 1 \end{pmatrix}$ —— (1)

Notice, $(x, y, z), (\tilde{x}, \tilde{y}, \tilde{z}) \in (\mathbb{F}_3)^3 \Rightarrow \begin{array}{l} x+\tilde{x} \in \mathbb{F}_3 \\ y+\tilde{y}+x\tilde{z} \in \mathbb{F}_3 \\ z+\tilde{z} \in \mathbb{F}_3. \end{array}$

$\therefore \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \tilde{x} & \tilde{y} \\ 0 & 1 & \tilde{z} \\ 0 & 0 & 1 \end{pmatrix} \in U(3, \mathbb{F}_3)$

For, $\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$ take $\begin{pmatrix} 1 & -x & xz-y \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{pmatrix}$,

(existance of unique Identity) $\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -x & xz-y \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -x & xz-y \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$

$= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ over field $\mathbb{F}_3$.

So, $U(3, \mathbb{F}_3)$ is a Group. And it's a subgroup of $SL_3(\mathbb{F}_3)$.

Now, we can clearly see that $U(3, \mathbb{F}_3)$ is not abalian. From ①

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & \tilde{x} & \tilde{y} \\ 0 & 1 & \tilde{z} \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \tilde{x}+x & y+\tilde{y}+x\tilde{z} \\ 0 & 1 & z+\tilde{z} \\ 0 & 0 & 1 \end{pmatrix}$$

by similer computation,

$$\begin{pmatrix} 1 & \tilde{x} & \tilde{y} \\ 0 & 1 & \tilde{z} \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \tilde{x}+x & y+\tilde{y}+\tilde{x}z \\ 0 & 1 & z+\tilde{z} \\ 0 & 0 & 1 \end{pmatrix}.$$

Now, $x\tilde{z} \neq \tilde{x}z \pmod 3$ $\forall$ $(x, \tilde{z}, z, \tilde{x}) \in (\mathbb{F}_3)^4$.

So, $U(3, \mathbb{F}_3)$ is not Abelian.

Take $A = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \in U(3, \mathbb{F}_3)$.

$$A^2 = \begin{pmatrix} 1 & 2a & 2b+ac \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{pmatrix}$$

$$A^3 = \begin{pmatrix} 1 & 2a & 2b+ac \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 3a & 3b+ac+2ac \\ 0 & 1 & 3c \\ 0 & 0 & 1 \end{pmatrix}.$$

$$= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{(taking mod 3)}.$$

So, $\forall$ $A \in U(3, \mathbb{F}_3)$, $A^3 = I$ but $U(3, \mathbb{F}_3)$ is not Abelian.

■