Name: Krishna Chaitanya Sripada

## Ans 1

To prove $O(n)$ is a group when equipped with the matrix multiplication, we need to prove that the 4 points mentioned in Definition 1 hold good.

**Point 1:** We need to prove that on multiplying two orthogonal matrices in $O(n)$, we get back an orthogonal matrix thus meaning the resultant matrix is also in $O(n)$.
Let us consider two orthogonal matrices G and H, then,

$(GG^T)(HH^T) = (GH)(G^T H^T) = (HG)(HG)^T = I$. This means that the resultant matrix is in the group $O(n)$.

**Proof by example:** $A_{n\times n}$ is an orthogonal matrix if, $AA^T = A^T A = I$. Consider the multiplication of following orthogonal matrices,

$$\begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = A$$

The transpose of this matrix is ,

$$A^T = \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Therefore,

$$AA^T = \begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = I$$

Also,

$$A^T A = \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = I$$

The resultant matrix also belongs to group $O(n)$.

**Point 2:** We need to prove that matrix multiplication of 3 matrices that belong to $O(n)$ is associative.
Let us consider three orthogonal matrices F, G and H, then,

$\sum_p \sum_q F_{ip} G_{pq} H_{qj} = \sum_p F_{ip}(\sum_q G_{pq} H_{qj}) = \sum_p F_{ip}(GH)_{pj} = F(GH)$
$\sum_p \sum_q F_{ip} G_{pq} H_{qj} = \sum_q (\sum_p F_{ip} G_{pq}) H_{qj} = \sum_q (FG)_{iq} H_{qj} = (FG)H$

**Point 3:** Let the element that belongs to the group $O(n)$ be an identity matrix (as Identity matrix is also orthogonal), then for another orthogonal matrix G $\in O(n)$, we get,

$G(I) = I(G) = G$. This is because matrix multiplication of an identity matrix and any other matrix is commutative in nature and returns the original matrix.

**Point 4:** We need to prove that the multiplication of an inverse and the matrix itself is an identity matrix which also belongs to the group $O(n)$.
Since, inverse of an orthogonal matrix is also orthogonal, it follows the Point 1 stated above where we check for the multiplication of two orthogonal matrices.
In this case, we get,
$G(G^{-1}) = I$ and $G^{-1}(G) = I$. Thus we can prove that the identity matrix also belongs to $O(n)$, we can say an inverse exists in $O(n)$.

## Ans 2

Since $U \in O(n)$, this means that U is in the group of orthogonal matrices, so for any matrix M that belongs to this group, we know that,

$M^T = M^{-1}$ (The transpose of M is the inverse of M).

Also, $MM^{-1} = I$

Therefore,

$MM^T = I$

Now taking a determinant on both sides, $det(MM^T) = detI$

We know that $detM * detM^T = 1$ (since $detI = 1$).

Now $detM * detM = 1$ (since $detM^T = detM$)

Meaning $(detM)^2 = 1$

Therefore, det(M) = ± 1.

## Ans 3

To prove $SO(n)$ is a subgroup of $O(n)$, we need to prove that the 2 points mentioned in Definition 2 hold good.

**Point 1:** To prove this, let us consider two orthogonal matrices G, H $\in SO(n)$, this means that the product of two orthogonal matrices should belong to the $SO(n)$.

**Proof by example:** Consider the multiplication of the following orthogonal matrices that below to $SO(n)$.

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix} = \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

The determinant of the resultant matrix = 1 which belongs to $SO(n)$ which is an special orthogonal matrix. Thus the resultant matrix also belongs to $SO(n)$.

**Point 2:** We need to prove that the inverse of a matrix and the multiplication of the same matrix is an identity matrix.

Since, inverse of an orthogonal matrix is also orthogonal, it follows the Point 1 stated above where we check for the multiplication of two orthogonal matrices.
In this case, we get,
$G(G^{-1}) = I$ and $G^{-1}(G) = I$. Thus we can prove that the identity matrix also belongs to $SO(n)$, we can say an inverse exists in $SO(n)$.

## Ans 4

Given that

$$e_1 = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

and $\mathcal{G} = \{U \in SO(n), Ue_1 = e_1\}$