Let G be a group and $|G|$ is finite
we define order of G, denoted by $o(G)$
to be equal to $|G|$.

- $o(\mathbb{Z}/n\mathbb{Z}) = n$
- $o(U(n)) = \phi(n)$ $\approx \varphi(n)$

08/08

Orthogonal Groups

Definition :

An $n \times n$ matrix A is said to be orthogonal if $AA^T = A^TA = I$

$$O_n(\mathbb{R}) = \{ A \in M_n(\mathbb{R}) \mid A \text{ is orthogonal} \}$$

claim :-

$O_n(\mathbb{R})$ is a group under matrix multiplication

i) Let $A, B \in O_n(\mathbb{R})$

$$(AB)(AB)^T = (AB)(B^TA^T) = (ABB^T)(A^T)$$
$$= AA^T = I$$

Similarly, $(AB)^T(AB) = I$

ii) Associativity is hereditary

iii) Since $I \in O_n(\mathbb{R})$, it has identity element

iv) Let $A \in O_n(\mathbb{R})$

Note that $I = (AA^T)^{-1} = (A^T)^{-1}A^{-1} = (A^{-1})^T(A^{-1})$

Similarly, $(A^{-1})(A^{-1})^T = I$

$\Rightarrow A^{-1} \in O_n(\mathbb{R})$

- Let $A \in O_n(\mathbb{R})$

$$A = \begin{pmatrix} | & | & & | \\ A_1 & A_2 & \cdots & A_n \\ | & | & & | \end{pmatrix} \qquad A^TA = \begin{pmatrix} & & \\ & a_{ij} & \\ & & \end{pmatrix}$$

$a_{ij} = A_i \cdot A_j$

$a_{ii} = A_i \cdot A_i = \|A_i\|^2$

$a_{ii} = 1 \Rightarrow \|A_i\| = 1$

$\Rightarrow A_i \cdot A_j = 0$ if $i \neq j$

$A_i \cdot A_j = 1$ if $i = j$

$\{A_1, \ldots, A_n\}$ is called an orthonormal basis of $\mathbb{R}^n$.

- Any $m \times n$ matrix A gives rise to a linear transformation $L_A : \mathbb{R}^n \longrightarrow \mathbb{R}^m$

$$u \longmapsto A \cdot u$$

- Let $A \in O_n(\mathbb{R})$. On $\mathbb{R}^n$, we have a usual dot product of vectors defined as

$$\underline{u} \cdot \underline{v} = u^T v$$

$u^T = (u_1, \ldots, u_n) \rightarrow$ transpose is row vector

$v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \rightarrow$ usual vector denotion is column vector

- Let $u, v \in \mathbb{R}^n$. Then

$$\begin{aligned} L_A(u) \cdot L_A(v) &= (Au) \cdot (Av) \\ &= (Au)^T (Av) \\ &= u^T A^T A v = u^T v \\ &= u \cdot v \end{aligned}$$

$\Rightarrow L_A$ preserves dot products in $\mathbb{R}^n$

$\Rightarrow L_A$ preserves norms in $\mathbb{R}^n$

? $\Rightarrow L_A$ preserves distance between two vectors

A function $f : \mathbb{R}^n \to \mathbb{R}^n$ is said to be an isometry if f preserves distance between any two points.

→ If $A \in O_n(\mathbb{R})$, then $L_A : \mathbb{R}^n \to \mathbb{R}^n$ is an isometry

For $n = 2$, let $A \in O_2(\mathbb{R})$

$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $\qquad$ $a^2 + c^2 = 1$, $b^2 + d^2 = 1$ $\qquad$ $ab + cd = 0$

$(\det(A))^2 = 1 \implies ad - bc = \pm 1$

let $(a, c) = (\sin\theta, \cos\theta)$ for some $\theta \in [0, 2\pi)$

$(\cos\theta, \sin\theta)$

Case - 1 : $ad - bc = 1$

$(\cos\theta)\, b + (\sin\theta)\, d = 0$

$(-\sin\theta)\, b + (\cos\theta)\, d = 1$

$\implies (b, d) = (-\sin\theta, \cos\theta)$

$$\implies A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

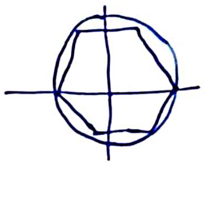
Case - 2 : $ad - bc = -1$

$$A = M_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$$

Exercise : Show that M_θ represents the reflection about the line joining $(0,0)$ and $(\cos\theta/2, \sin\theta/2)$

Dihedral group

Let us consider a regular n-gon inscribed in a unit circle, with one of the vertices at $(1, 0)$



Let T denote the rotation of the plane counter-clock wise by an angle $2\pi/n$

$$T = \begin{pmatrix} \cos \frac{2\pi}{n} & -\sin \frac{2\pi}{n} \\ \sin \frac{2\pi}{n} & \cos \frac{2\pi}{n} \end{pmatrix}$$

$$T^n = I$$

$$T^i = \begin{pmatrix} \cos \frac{2\pi i}{n} & -\sin \frac{2\pi i}{n} \\ \sin \frac{2\pi i}{n} & \cos \frac{2\pi i}{n} \end{pmatrix}$$

$\Rightarrow$ $I, T, T^2, \ldots, T^{n-1}$ are all distinct

- $T^i \cdot T^j = T^{(i+j) \bmod n}$

- Let S represent the reflection about X-axis

$$S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad S^2 = I \qquad S \neq I$$

$S \neq T^i$ for any i

★ $TS = ST^{-1} = ST^{n-1}$

Proof :- $(\theta = 2\pi/n)$

$$TS = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$$

$$ST^{n-1} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \cos\theta(n-1) & -\sin\theta(n-1) \\ \sin(\theta(n-1)) & \cos(\theta(n-1)) \end{pmatrix}$$

$$= \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$$

$\Rightarrow$ $TS = ST^{n-1}$

$TS = ST^{-1}$

$T^2 S = T(TS)$

$T^2 S = T(ST^{-1}) = ST^{-2}$

- Define D_{2n} as follows

- $D_{2n} = \{I, T, T^2, \ldots, T^{n-1}, S, ST, ST^2, \ldots, ST^{n-1}$

showing that D_{2n} is a group

$\rightarrow$ (closed) $T^i T^j = T^{(i+j) \bmod n} \in D_{2n}$

$(ST^i)(ST^j) = S(T^iS)T^j = SST^{-i}T^j$
$= T^{j-i} \in D_{2n}$

$T^i ST^j \in D_{2n}, \quad ST^iT^j \in D_{2n}$

$\rightarrow$ (Inverse) $(T^i)^{-1} = T^{-i} = T^{n-i}$

$(ST^i)^{-1} = T^{-i}S^{-1} = T^{-i}S = T^{n-i}S$
$= ST^{i-n} = ST^i$

D_{2n} is called a Dihedral group of order $2n$.

The Heisenberg Group

Let F be a field

$F = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}$ are examples of fields

Let $H(F) = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \middle| \; a, b, c \in F \right\}$

Claim : $H(F)$ is a group under matrix multiplication

Check that

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

$H(F)$ is called the Heisenberg group

Quaternions

$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad i = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix} \quad j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

$K = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$

$Q_8 = \{\pm I, \pm i, \pm j, \pm K\}$