$i^2 = -I$, $j^2 = -I$, $k^2 = -I$

$ij = k = -ji$

$jk = i = -kj$

$ki = j = -ik$

Exercise :

Check that Q_8 is non Abelian group under multiplication

11/08

Definition

A function $m : \mathbb{R}^n \to \mathbb{R}^n$ is called as isometry of $\mathbb{R}^n$ if $\| m(u) - m(v) \| = \| u - v \|$

Examples

(i) If A is an orthogonal matrix, then $u \to Au$ is an isometry

(ii) Let $t_w : \mathbb{R}^n \to \mathbb{R}^n$ be given by $u \mapsto u + w$ where w is a fixed element in $\mathbb{R}^n$

$\| t_w(u) - t_w(v) \| = \| (u+w) - (v+w) \| = \| u - v \|$

Remark

Let $M_n = \{ m : \mathbb{R}^n \to \mathbb{R}^n \mid m \text{ is an isometry} \}$

1. closed

If $m_1, m_2 \in M_n$

$= \| m_1 \circ m_2(u) - m_1 \circ m_2(v) \|$

$= \| m_2(u) - m_2(v) \|$ [Because of isometry poperty of m_1]

$= \| u - v \|$

2. Associativity is hereditary

3. $Id : \mathbb{R}^n \to \mathbb{R}^n$ is an isometry

4. Let $f \in M_n$

f is injective

If $f(u) = f(v)$ $\Rightarrow \| f(u) - f(v) \| = 0$

$\Rightarrow \| u - v \| = 0$ $\Rightarrow$ $u = v$

Theorem

Let $m: \mathbb{R}^n \to \mathbb{R}^n$ be any function. Then the following are true (equivalent)

i) m is an isometry and $m(0) = 0$

ii) m preserves dot products i.e if $u, v \in \mathbb{R}^n$, then $m(u) \cdot m(v) = u \cdot v$

iii) m is given by an orthogonal linear transformation i.e $m(u) = Au$ for some $A \in O_n(\mathbb{R})$

Lemma

Let $f: \mathbb{R}^n \to \mathbb{R}^n$ be a function satisfying

i) $f(u) f(v) = u \cdot v$

ii) $f(e_i) = e_i$ where $e_i = (0, 0, \dots, 1, 0, \dots 0)$ ($\uparrow$ i^{th} position)

Then $f = Id$

To show that $f(u_1, u_2, \dots, u_n) = (u_1, \dots, u_n)$ $\forall u \in \mathbb{R}^n$

We want to prove that

$$f(u) \cdot e_i = u \cdot e_i \quad \forall i$$

But $f(u) \cdot e_i = f(u) \cdot f(e_i)$

$= u \cdot e_i$ [From Theorem]

Proof for Theorem

(a) $\Rightarrow$ (b)

$$\|u - v\|^2 = u \cdot u - u \cdot v - v \cdot u + v \cdot v$$

$$\|m(u) - m(v)\|^2 = m(u) \cdot m(u) - m(u) \cdot m(v) - m(v) \cdot m(u) + m(v) \cdot m(v)$$

Using (a), $\|m(u)\|^2 = \|u\|^2$

$\Rightarrow$ $2 u \cdot v = 2 m(u) \cdot m(v)$ [$u \cdot v = v \cdot u$]

$\Rightarrow$ $\boxed{u \cdot v = m(u) \cdot m(v)}$

✱ (b) $\Rightarrow$ (c)

Let us define $A = \begin{pmatrix} | & | & & | \\ m(e_1) & m(e_2) & \cdots & m(e_n) \\ | & | & & | \end{pmatrix}$

Let $A^T A = \begin{pmatrix} a_{ij} \end{pmatrix}$, then $a_{ij} = m(e_i)\, m(e_j)$

Thus $A^T A = Id = AA^T = \begin{cases} 1 & \text{if } i=j \\ 0 & \text{if } i \neq j \end{cases}$

because $m(e_i) \cdot m(e_j) = e_i \cdot e_j$

$\Rightarrow A_n \in O_n(\mathbb{R})$

Let $L : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ be the orthogonal linear transformation given by

$$L : \mathbb{R}^n \longrightarrow \mathbb{R}^n$$
$$u \longmapsto A^{-1} u$$

L, m preserve dot products

Hence $L \circ m$ preserves dot products

Now, $L \circ (m(e_i)) = L(Ae_i) = A^{-1}(Ae_i) = e_i$

By the Lemma $L \circ m = Id$ i.e, $\forall\, u \in \mathbb{R}^n$

$$L \circ (m(u)) = u$$

$$A^{-1}(m(u)) = u \quad \Rightarrow \quad m(u) = Au$$

(c) $\Rightarrow$ (a)

$m(u) = Au$, $A \in O_n(\mathbb{R})$

$\| m(u) - m(v) \| = \| Au - Av \| = \|A\| \, \|u - v\| = \|u - v\|$

$m(0) = A \cdot \underline{0} = 0$

Hence, (a), (b), (c) are all equivalent

Theorem (Structure theorem for isometry)

Let $m : \mathbb{R}^n \to \mathbb{R}^n$ be an isometry. Then there exists $A \in O_n(\mathbb{R})$ and $w \in \mathbb{R}^n$ such that

$m(u) = Au + w$

Proof : For $w \in \mathbb{R}^n$, let $t_w : \mathbb{R}^n \to \mathbb{R}^n$ given by $t_w(u) = u + w \quad \forall\, u \in \mathbb{R}^n$

Let $m : \mathbb{R}^n \to \mathbb{R}^n$ be an isometry

Suppose $m(0) = w$

Consider the map $t_{-w} \circ m$

Now, $t_{-w}(m(0)) = t_{-w}(w)$

$= w - w = 0$

By the above theorem,

* $t_{-w}(m(0)) = Au$ [From (c) of Theorem]

But $t_{-w}(m(u)) = m(u) - w$

$\Rightarrow m(u) = Au + w$

Given $A \in M_n(\mathbb{R})$, we define $T_A : \mathbb{R}^n \to \mathbb{R}^n$ by $T_A(u) = Au$

The last theorem shows that if $f : \mathbb{R}^n \to \mathbb{R}^n$ is an isometry, then $f = t_{+w} \circ T_A$ for some $A \in O_n(\mathbb{R})$ and $w \in \mathbb{R}_n$

Thus, if f is an isometry given by $f = t_w \circ T_A$ then f is a bijection and hence f^{-1} exists.

Now $f^{-1} = (t_w \circ T_A)^{-1} = T_A^{-1} \circ t_{-w}$ is an isometry

$\Rightarrow M_n$ is a group

- $T_A^{-1}(t_{-w}(u)) = t_{-A^{-1}w}\, T_{A^{-1}}(u)$

Subgroups

Let G be a group. A subset H of G is called a subgroup of G if H itself is a group.

Notation

$H \leq G \rightarrow$ Denotes H is a subgroup of G

Examples

i) $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$

ii) $(-1, 1) \leq (\mathbb{Q}^{\times}, \cdot) \leq (\mathbb{R}^{\times}, \cdot) \leq (\mathbb{C}^{\times}, \cdot)$

iii) $S^1 = \{ z \in \mathbb{C} \mid |z| = 1 \}$

$(S^1, \cdot) \leq (\mathbb{C}^{\times}, \cdot)$

iv) $SL_n(\mathbb{C}) \leq GL_n(\mathbb{C})$

$SO_n(\mathbb{R}) \leq O_n(\mathbb{R}) \leq GL_n(\mathbb{R})$

v) $\{ e^{\frac{2\pi i}{n}} \mid i = 0, \ldots, n-1 \} \leq (S^1, \cdot)$

Proposition

Let G be a group and $H \subseteq G$

(i) $H \leq G$

(ii) $H \neq \emptyset$ and for $x, y \in H$, $xy \in H$ and $x^{-1} \in H$

(iii) $H \neq \emptyset$ and for $x, y \in H$, $xy^{-1} \in H$

Proof:

a $\Rightarrow$ b Follows from definition

b $\Rightarrow$ c For $y \in H$, we have $y^{-1} \in H$

Also, for $x, y^{-1} \in H$, we have $xy^{-1} \in H$

c $\Rightarrow$ a Since $H \neq \emptyset$, $\exists\, x \in G$ such that $x \in H$

$\Rightarrow x x^{-1} \in H \Rightarrow e \in H$

Let $y \in H$, then $ey^{-1} \in H \Rightarrow y^{-1} \in H$