Let $x, y \in H$. Then $x, y^{-1} \in H$. By point ⓒ

$$xy = x(y^{-1})^{-1} \in H$$

18/08

Proposition

If H is a subgroup of $\mathbb{Z}$, then there exists $m \in \mathbb{Z}$ such that $H = m\mathbb{Z}$

- Let H be a subgroup of $\mathbb{Z}$

case – (i) : $H = (0) = 0\mathbb{Z}$

case – (ii) : $H \neq (0)$

$\Rightarrow$ There exists an element $k \in \mathbb{Z} \setminus \{0\}$ such that $k \in H$

We claim that $H_{>0} = \{k \in \mathbb{Z} \mid k > 0, k \in H\} \neq \emptyset$

Define $m := \min H_{>0}$

$m\mathbb{Z} \subseteq H \longrightarrow$ trivial from closure

$m, m+m, \ldots, -m, -m-m, \ldots, 0$ are all part of H

$H \subseteq m\mathbb{Z} \longrightarrow$ Let $a \in H$

By remainder theorem, $\exists\, q, r \in \mathbb{Z}$ with $0 \leq r < m$ such that

$a = mq + r$

$r = a - mq \in H$

By minimality of m, we have $r = 0$

$\Rightarrow a = mq \in m\mathbb{Z}$

$\Rightarrow H \subseteq m\mathbb{Z}$

Definition

Let G be a group and $x \in G$. We define the cyclic group generated by x to be the smallest subgroup of G that contains x.

This is denoted by $\langle x \rangle$

- If $o(x)$ is infinite, then $\langle x \rangle = \{\dots x^{-2}, x^{-1}, 1, x, x^2, \dots\}$

- If $o(x) = n$, then $\langle x \rangle = \{1, x, x^2, \dots, x^{n-1}\}$

Proposition

Let H be a finite subgroup of $O_2(\mathbb{R})$.

Then

(i) $H = C_n$; a cyclic group of order n

(ii) H is a dihedral group

Pf : If $H = (id)$, nothing to prove.

So, $H \neq (id)$

Case-(i) : H consists of only finitely many rotations

$H = \langle \rho_{2\pi/n} \rangle$, where for any θ; ρ_θ is the rotation by an angle θ anticlockwise and $n = |H|$

Proof : Let θ be the smallest positive angle such that $\theta \in H$

Then $\langle \rho_\theta \rangle \subseteq H$

Let $\rho_\alpha \in H$, then there exists $q, r \in \mathbb{Z}$ such that $\alpha = q\theta + r$, where $0 \le r < \theta$

$r = \alpha - q\theta \in H \Rightarrow \rho_r = \rho_\alpha (\rho_\theta)^{-q} \in H$

By minimality of θ, $r = 0$

$\Rightarrow \rho_\alpha = (\rho_\theta)^q$

$\Rightarrow$ But $(\rho_\theta)^q \in \langle \rho_\theta \rangle$

$\Rightarrow H \subseteq \langle \rho_\theta \rangle$

$\Rightarrow \theta = \frac{2\pi}{n}$

So, for finitely many rotations, H is a cyclic group of order n.

Case - 2 :- There exists reflections $r' \in H$ where r' is reflection about some line ℓ.
After a change of coordinates, if necessary, we may assume that ℓ is x-axis.

Let $H' = H \cap SO_2 \leq O_2(\mathbb{R})$ $[SO_2(\mathbb{R}) \leq O_2(\mathbb{R})]$

By case-1, $\exists\, \theta$ such that $H' = \langle \rho_\theta \rangle$

Let $g \in H \setminus SO_2(\mathbb{R})$

Then $gr \in H'$

$\Rightarrow g = gr^2 = (gr)r \in H_r'$ where

$H_r' = \{ kr \mid h \in H' \}$

$H = H' \cup H_r'$

$= \{1, \rho_\theta, \dots, \rho_\theta^{|H|-1}\} \cup \{r, \rho_\theta r, \dots, \rho_\theta^{|H|-1} r\}$

$= D_{2|H'|}$

Definition

Let G be a group.

i) The centre of G, denoted by $Z(G)$ is defined as $Z(G) = \{ x \in G \mid xy = yx \ \ \forall y \in G \}$

ii) For $a \in G$, the centraliser of a, denoted by $C(a)$ is given by $C(a) = \{ x \in G \mid xa = ax \}$

Pf: $Z(G) \subseteq C(a) \quad \forall a$

$$Z(G) = \bigcap_{a \in G} C(a)$$

Proposition

$Z(G) \leq G$ and $C(G) \leq G$

Pf: Since $1 \in C(a)$, we have $C(a) \neq \emptyset$

Let $x, y \in C(a)$. Then $a(xy) = (ax)y = (xa)y$

$= x(ay)$

$= x(ya)$

$= (xy)a$

Let $x \in C(a)$

Then $ax = xa$

$x^{-1}axx^{-1} = x^{-1}xax^{-1}$

$\Rightarrow x^{-1}a = ax^{-1}$

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

$\Rightarrow C(G) \leq G$

countable intersection maintains subgroup property

$\Rightarrow Z(G) \leq G$

- $Z(D_8) = \{1, r^2\}$

$\rightarrow D_8 = \{1, r, r^2, r^3, sr, s, sr^2, sr^3\}$

and $rs = sr^3$

$r^2 s = sr^2 \longrightarrow r^3 sr = rsr^3$

$r^2 s = r^2 s$ ✓

Cyclic groups

(i) $(\mathbb{Z}, +)$

(ii) $(\mathbb{Z}/n\mathbb{Z}, +)$

(iii) $U_n \rightarrow$ not cyclic in general

* check $H = \left\langle \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle$

Proposition

Let G be a group and $a \in G$

If $a^m = a^n = 1$, then $a^{\gcd(m,n)} = 1$

In particular, $o(a) \mid m$ wherever $a^m = 1$

Proof :

Let $d = \gcd(m,n)$

There exist $x, y \in \mathbb{Z}$ such that $mx + ny = d$

Then $a^d = a^{mx+ny} = (a^m)^x (a^n)^y = 1$

Let $d = o(a)$

Then $a^d = 1 = a^m$

$\Rightarrow a^{\gcd(d,m)} = 1$

$\Rightarrow d \leq \gcd(d,m) \leq d$

$\Rightarrow d = \gcd(d,m)$

$\Rightarrow d \mid m$

Proposition

Let $H = \{1, x, x^2, \ldots, x^{n-1}\}$

Then $o(x^a) = \dfrac{n}{\gcd(a,n)}$

- Let $d = \gcd(a,n)$

  $o(x) = n$

  $\Rightarrow x^n = 1$

  $\Rightarrow x^{an} = 1$

- $(x^a)^{n/d} = (x^n)^{a/d}$

  $\Rightarrow m \mid n/d$

- Suppose $m = o(x^a)$

  $\Rightarrow (x^a)^m = 1$

  $\Rightarrow n \mid am$

  $\Rightarrow \frac{n}{d} \mid \frac{am}{d}$

  $\Rightarrow \frac{n}{d} \mid m$