Dihedral Groups

Let $n \geq 3$, $n \in \mathbb{Z}$

The group given by the symmetries of a regular n-gon is called a Dihedral group, written D_n

$D_3 = \{ R_0, R_{120}, R_{240}, F_V, F_L, F_R \}$ symmetries of a triangle

$|D_3| = 6$ order of D_3

What is $|D_n|$ if $n \geq 3$? Excercise 5, chapter 1

Which of D_n $(n \geq 3)$ are abelian? Excercise 14, chapter 1

In D_3

We know that $R_{120}^2 = R_{240}$

Also that $R_{120} F_V = R_{120} \circ F_V = F_R$

$R_{120}^2 F_V = F_L$

⑥ $D_3 = \{ R_{120}^3, R_{120}, R_{120}^2, F_V, R_{120}^2 F_V, R_{120} F_V \}$

We say that D_3 is generated by R_{120} and F_V, and using these properties, any expression involving R_{120} and F_V can be simplified into one of the ⑥ above.

Ex 13, $G = D_3$, Let $R = R_{120}$, $F = F_v$, write $(R^4F)R^2$ as one of the ⑥

$(R^4F)R^2 = (R^3RF)R^2 = (RF)R^2$ $\qquad F_v R_{120} = R_{120}^{\,2} F_v$

$= R(FR)R$

$= R(R^2F)R$

$= RR^2(FR)$

$= R^3(R^2F)$

$= R^2F$

Finite groups and subgroups

Note: $R_{120}^3 = R_0 =$ identity

We say the order of R_{120} is 3

If g is an element of a group G and $g^n = e$ where n is the smallest positive integer with this property, then we say, the order of g is n, written $|g|$.

If no such integer exists, then g has infinite order

Example 14 Find the order of these elements

a) F_v in D_3 $\qquad F_v^{\,2} = R_0$ so $|F_v| = 2$

b) R_{240} in D_3 $\qquad 3$

c) 4 in $\mathbb{Z}_6$ $\qquad 4 \neq 0$, $4^2 = 4+4 \neq 0$ $\qquad \mathbb{Z}_6 = \{0, 1, \ldots, 5\}$ + mod 6

$e = 0$ $\qquad 4^3 = 4+4+4 = 12 \equiv 0$, $|4| = 3$

d) 7 in $U(15)$ $\qquad 7 \neq 1$, $7^2 = 49 \equiv 4 \neq 1$, $7^3 \equiv 4 \cdot 7 = 28 \equiv 13 \neq 1$

$e = 1$ $\qquad 7^4 \equiv 4 \cdot 4 \equiv 16 \equiv 1$. so $|7| = 4$

e) 2 in $(\mathbb{Z}, +)$ $2 \neq 0$, $2^2 = 2+2 = 4 \neq 0$

$e = 0$ $2^3 = 2+2+2 = 6 \neq 0$, never 0

$|2|$ has infinite order

Example 15 Let G be a group and $a \in G$ and a has finite order. Prove that $|a| = |a^{-1}|$

Suppose $|a| = n$, ie n is the smallest positive integer such that $a^n = e$.

$$(a^{-1})^n = (a^{-1})^n e = (a^{-1})^n a^n = \underbrace{a^{-1}a^{-1}\dots a^{-1}}_{n \text{ times}} \underbrace{a\,a\dots a}_{n \text{ times}}$$

$$= \dots = e \qquad \therefore (a^{-1})^n = e$$

We must now show that no smaller positive integer could work

Suppose $k \in \mathbb{Z}^+$ and $(a^{-1})^k = e$ and $k < n$

$$\Rightarrow a^k = a^k e = a^k (a^{-1})^k = \underbrace{aa\,aa\dots a}_{k \text{ times}} \underbrace{a^{-1}a^{-1}a^{-1}a^{-1}\dots a^{-1}}_{k \text{ times}}$$

$$= \dots = e \qquad \therefore a^k = e$$

Contradiction since $|a| = n$, hence $|a^{-1}| = n$.

Rotations

What do we get if we consider only the rotations within D_3?

$D_3 = \{ R_0, R_{120}, R_{240}, F_V, F_L, F_R \}$

Let $H = \{ R_0, R_{120}, R_{240} \}$

H is a group within another group

Subgroups

If H is a subset of a group G, and H itself is a group under the same operation as G, then H is a subgroup of G, written $H \leq G$.

Example 16

$H = \{ R, R_{120}, R_{240} \}$ is a subgroup of D_3

Example 17

Is $(\{-1, 1\}, \times)$ a subgroup of $(\mathbb{Z}, +)$?

$\{-1, 1\}$ is a subset of $\mathbb{Z}$ $\quad (G, *)$

$(\{-1, 1\}, \times)$ is a group but operation is different so not a subgroup.

Remarks

1) Every group is a subgroup of itself.

2) For any group G, $\{e\}$ is a subgroup of G.

Definition

- We write $H < G$ is, H is a subgroup of G but $H \neq G$. Then H is a proper subgroup of G.
- $\{e\}$ is called the trivial subgroup of G.

H in Ex⑯ is a proper, nontrivial subgroup of D_3

Example 18

Consider $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ addition modulo 6, we know its a group and its inverses are in Week 2.

Is $\{0, 1, 5\}$ a subgroup?

$1+1=2 \notin H$, $\therefore$ it is not closed $\Longrightarrow$ it is not a subgroup

Can you find other subgroups of $\mathbb{Z}_6$?

$H_1 = \{0, 3\}$

$H_2 = \{0, 2, 4\}$

$H_3 = \{0\}$

$H_4 = \mathbb{Z}_6$

Proposition 9

Two-step subgroup test, let G be a group and H is a subset of G

If:

- H is a non-empty subset of a
- $a, b \in H \Rightarrow ab \in H$
- $a \in H \Rightarrow a^{-1} \in H$

then H is a subgroup of G

Proof

Suppose H has these properties, want to show that H is a group.

- Closure

  This is property ii

- Associativity

  If we're using the same operation as G, then we know its associative

- Identity

  By (i), $H \neq \emptyset$ so say $g \in H$

  (iii) $\Rightarrow g^{-1} \in H$ so then by (ii) $gg^{-1} \in H$ and $gg^{-1} = e$ so $e \in H$

- Inverse

  Same as identity

So it is a group ■

Proposition 10

One Step Subgroup test, suppose G is a group, If:

- H is a non-empty subset of G
- $a, b \in H \rightarrow ab^{-1} \in H$

Proof Exercise, page 62

Proposition 11

There is a finite subgroup test in the book, page 64

Example 19

Consider $(\mathbb{Z}, +)$ and define H to be the set of even integers under addition. Is this a subgroup of $(\mathbb{Z}, +)$?

One Step

i) $H \subseteq \mathbb{Z}$, and $2 \in H$, $3678 \in H$ ✓

ii) Let $a, b \in H$ so a, b are even. Then $ab^{-1} = a + (b^{-1}) = a - b$

$a - b$ is even so $a - b \in H$. So H is a subgroup of $(\mathbb{Z}, +)$.

Two Step

i) as before

ii) Let $a, b \in H$, so a, b is even and $a + b$ is even, so $a + b \in H$

ii) If $a \in H$, a is even. Then a^{-1} ie $-a$ is even so $-a \in H$

So H is a subgroup

Example 20

Is $H = \{a + bi \mid a, b \in \mathbb{R}, a \geq b\}$ a subgroup of $(\mathbb{C}, +)$?

Two Step

i) $H \subseteq \mathbb{C}$, $0 \in H$ and $3 + i \in H$

ii) Suppose $a + bi \in H$ and $c + di \in H$ so $a, b, c, d \in \mathbb{R}$ and $a \geq b$, $c \geq d$. Then $(a + bi) + (c + di) = (a + c) + (b + d)i$

$a + c \geq b + d$, so $(a + c) + (b + d)i \in H$

iii) Inverse Suppose $a + bi \in H$ so $a \geq b$, then

$(a + bi)^{-1} = -a - bi$ $\quad -a \leq -b$ $\quad \notin H$ $\quad \therefore$ Not a subgroup

Example 21

Is $H = \{a + bi \mid a,b \in \mathbb{R},\ a \neq b\}$ a subgroup of $(\mathbb{C}, +)$?

$2 + i \in H$

$1 + 2i \in H$ but $(2+i)+(1+2i) = 3 + 3i \notin H$

No closure, H is not a subgroup

Definition

Let G be a group. Then the centre $Z(G)$ of G is defined by

$$Z(G) = \{a \in G \mid ax = xa \text{ for all } x \in G\}$$

The set of elements in G that commute with all elements in G.

Example 22

Suppose G is abelian, what is $Z(a)$?

Abelian: if $a,b \in G$ then $ab = ba$. Then all of G is in $Z(a)$ ie $Z(G) = G$

Definition

Let $a \in G$. Then the centralizer of a in G written $C(a)$ is

$$C(a) = \{g \in G \mid ga = ag\}$$

The set of elements in G that commute with a.

Example 23

Find the centralizer of $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ in $GL(2, \mathbb{R})$

Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \mathbb{R})$ $a,b,c,d \in \mathbb{R}$ and $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in C\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ iff $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & -a \\ d & -c \end{pmatrix} \qquad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}$$

Want them to be equal

$b = -c$ $\qquad -a = -d$

$d = a$ $\qquad -c = b$

So $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

Answer: $C\left(\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right) = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R},\ a^2 + b^2 \neq 0 \right\}$

Remark $Z(GL(3,\mathbb{R})) = I\begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}$, Diagonal $\begin{pmatrix} a & a & 0 \\ 0 & a & a \end{pmatrix}$

$= \{kI \mid k \in \mathbb{R}^*\}$ Exercise

Example

a) Find the centralizers of each of the elements in D_3

$C(R_0) = D_3$

$C(R_{120}) = \{R_0, R_{120}, R_{240}\}$

$C(R_{240}) = \{R_0, R_{120}, R_{240}\}$

$C(F_v) = \{R_0, F_v\}$

$C(F_R) = \{R_0, F_R\}$

$C(F_L) = \{R_0, F_L\}$

b) Find $Z(D_3) = \{R_0\}$

Find $Z(D_N)$ page 67

Theorem 12

Let G be a group with an element $a \in G$. Then $C(a)$ is a subgroup of G.

Two Step

i) $C(a) = \{ g \in G \mid ag = ga \}$, $C(a) \subseteq G$

$aa = aa$ so $a \in C(a)$, same with e, so $C(a) \neq \emptyset$

ii) Closure $g, h \in C(a)$ so $ga = ag$, want to show $gh \in C(a)$ and that $(gh)a = a(gh)$

$(gh)a = g(ha) = g(ah) = (ga)h = (ag)h = a(gh)$

$\therefore gh \in C(a)$

iii) Suppose $g \in C(a)$, so $ga = ag$, WTS $g^{-1} \in C(a)$ and $g^{-1}a = ag^{-1}$

$g^{-1}(ga) = g^{-1}(ag) \Rightarrow a = g^{-1}ag \Rightarrow ag^{-1} = g^{-}a\,\cancel{gg^{-1}} \Rightarrow ag^{-1} = g^{-1}a$

So $g^{-1} \in C(a)$

Hence $C(a)$ is a subgroup