TRY

- 1. Show that G={1,-1,i,-i} is a group under usual multiplication.
- 2. If * is defined on R such that a*b=a+b-ab, for a,b $\in$ R, show that (R,*) is an abelian group.
- 3. If * is defined on Q^+ such that a*b=ab/3, for a,b $\in$ Q^+, show that {Q^+,*} is an abelian group.
- 4. Show that the following sets of 2X2 matrices form a group under matrix multiplication

$$i) G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$$

(3) $(Q^+, *)$.

$$a * b = \frac{ab}{3} \quad \forall\ a, b \in Q^+$$

Closure $\quad a * b = \frac{ab}{3} \in Q^+$

Q^+ is closed under $*$

Associative $\quad a * (b * c) = a * \left(\frac{bc}{3}\right) = \frac{a \times \frac{bc}{3}}{3}$

$$a * (b * c) = \frac{abc}{9}$$

$$(a * b) * c = \left(\frac{ab}{3} * c\right) = \frac{\frac{ab}{3} \times c}{3} = \frac{abc}{9}$$

$$\therefore a * (b * c) = (a * b) * c \quad \forall\ a, b, c \in Q^+$$

Identity Let $e \in \mathbb{Q}^+$ be the identity

Then $a * e = a = e * a \quad \forall a \in \mathbb{Q}^+$

$a * e = a \Rightarrow \frac{ae}{3} = a \Rightarrow e = 3$

$e * a = a \Rightarrow \frac{ea}{3} = a \Rightarrow e = 3$

$\therefore e = 3$ is the identity for $\mathbb{Q}^+$ under $*$

Inverse Let $a^{-1} \in \mathbb{Q}^+$ be the inverse of a. Then $a * a^{-1} = a^{-1} * a = e = 3$

$a * a^{-1} = 3 \Rightarrow \frac{aa^{-1}}{3} = 3 \Rightarrow a^{-1} = 9/a$

$$a^{-1} * a = 3 \Rightarrow \frac{a^{-1}a}{3} = 3 \Rightarrow a^{-1} = \frac{9}{a}$$

$$\forall\ a \in Q^+, \quad a^{-1} = \frac{9}{a}$$

Also $a * b = \frac{ab}{3} = \frac{ba}{3} = b * a$

$\therefore$ Q^+ is an abelian group under $*$

④ $G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$

A B C D

$\begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix}$

matrix mult	A	B	C	D
A	A	B	C	D
B	B	A	D	C
C	C	D	A	B
D	D	C	B	A

$B \times B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = A$

$B \times C = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = D$

$B \times C = C \times B = D$

$B \times D = D \times B = C$

$C \times D = D \times C = B$

$B \times B = A$

$C \times C = A$

$D \times D = A$

(5) $G = \{2, 4, 6, 8\}$ under multiplication module 10 $[\times_{10}]$

$$a \times_{10} b = (ab) \bmod 10$$

$\times_{10}$	2	4	6	8
2	4	8	2	6
4	8	6	4	2
6	2	4	6	8
8	6	2	8	4

$2 \times_{10} 2 = 4 \bmod 10$
$= 4$

$2 \times_{10} 4 = 8 \bmod 10$
$= 8$

$2 \times_{10} 6 = 12 \bmod 10$
$= 2$

From the Cayley table, it is obvious that G is closed under $\times_{10}$.

$a \times_{10} (b \times_{10} c) = (a \times_{10} b) \times_{10} c \quad \forall a, b, c \in G$

$\times_{10}$ is associative

6 is the identity element which is obvious from 3rd row and 3rd column.

$2 \times_{10} 6 = 6 \times_{10} 2 = 2, \quad 4 \times_{10} 6 = 6 \times_{10} 4 = 4$

$8 \times_{10} 6 = 6 \times_{10} 8 = 8, \quad 6 \times_{10} 6 = 6$

Inverse of 2 is 8 For $2 \times_{10} 8 = 8 \times_{10} 2 = 6$

Inverse of 4 is 4. For $4 \times_{10} 4 = 6$

Inverse of 6 is 6 For $6 \times_{10} 6 = 6$

Also $a \times_{10} b = b \times_{10} a \quad \forall a, b \in G$

$\therefore G = \{2, 4, 6, 8\}$ is a group under $\times_{10}$

To find the order of every element in $(Z_6, +_6)$

$Z_6 = \{0, 1, 2, 3, 4, 5\}$

Order of 0 is 1

$1 +_6 1 +_6 1 +_6 1 +_6 1 +_6 1 = 0 \Rightarrow o(1) = 6$

$2 +_6 2 +_6 2 = 0$

$4 +_6 4 +_6 4 = 0$

$5 +_6 5 +_6 5 +_6 5 +_6 5 +_6 5 = 0$

$(G, *)$

$H \subseteq G$

$a, b \in H.$

$a * b^{-1} \in H$

$Z_4 = \{0, 1, 2, 3\}$ is a group under $+_4$.

Let $H = \{0, 2\}$. To prove H is a subgroup of Z_4 under $+_4$

Now $a \in H$

$0 +_4 2^{-1} = 0 +_4 2 = 2 \in H$

$\therefore (H, +_4)$ is a subgroup of $(Z_4, +_4)$

n m

$(G, *)$ $(H, *)$

$(R, +)$ $(Q, +)$

Example for finite group

Klein's 4 group

$G = \{e, a, b, c\}$ [Felix Klein]

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$e * e = e$
$a * a = e$
$b * b = e$
$c * c = e$

$b * a = a * b = c$

$c * a = a * c = b$

$b * c = c * b = a$

From the table it is clear that G is closed under $*$. Associative property holds good. e is the identity. e, a, b, c are self inverses. Also $a * b = b * a \; \forall \; a, b \in G$

$\therefore$ G is an abelian group.

e, a, b, c

a, b, c

$a * (b * c) =$

$a * (c * b) =$

$b * (c * a) =$

$b * (a * c)$

$c * (a * b)$

$c * (b * a,$

e, a, b

Elementary properties of groups

Lemma 3 *Let $(G,*)$ be a group. Then*

1. *the identity element e_G of $(G,*)$ is unique; and*
2. *for each $x \in G$, the inverse $\bar{x}$ of x in $(G,*)$ is unique.*
3. (Cancellation laws) *If $a,b,c \in G$ with $a*c = b*c$, then $a = c$. Similarly, if $x,y,z \in G$ with $z*x = z*y$, then $x = y$.*

Proof.

1. If e, f are two identity elements for $(G, *)$, then $e * f = e$ since f is an identity element, while $e * f = f$ since e is an identity element. Hence $e = e * f = f$.

2. Suppose that $y, z \in G$ are inverses for $x \in G$ in $(G, *)$. Then $y = y * e_G = y * (x * z) = (y * x) * z = e_G * z = z$.

3. Let $\bar{c}$ be the inverse of c in $(G, *)$. If $a * c = b * c$, then $a = a * e_G = a * (c * \bar{c}) = (a * c) * \bar{c} = (b * c) * \bar{c} = b * (c * \bar{c} = b * e_G = b$. The second statement is proved in a similar way.

Definition. A *subgroup* of a group $(G, *)$ is a subset of G which is also a group with respect to (the restriction of) the same binary operation $*$ as in G.

Remark. In particular, if H is a subgroup of $(G, *)$, then the restriction of $*$ is a binary operation on H, in other words H is closed with respect to $*$.

Examples.

1. $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are subgroups of $(\mathbb{C}, +)$.

2. If n is a positive integer, then the set $n\mathbb{Z} := \{nk; k \in \mathbb{Z}\}$ of all multiples of n is a subgroup of $(\mathbb{Z}, +)$.

3. The special linear group $SL_n(\mathbb{R})$ of $n \times n$ matrices with real entries and determinant 1 is a subgroup of the general linear group $GL_n(\mathbb{R})$ of all invertible $n \times n$ matrices with real entries.

4. We can regard the group S_n of permutations of the set $\{1, 2, \ldots, n\}$ as a subgroup of the set S_{n+1} of permutations of the set $\{1, 2, \ldots, n, n+1\}$, namely those permutations $\sigma \in S_{n+1}$ for which $\sigma(n+1) = n+1$.

(i) $(G, *)$ is a group. H is a subset of G.

It is enough to check closure and inverse.

$a, b \in H \Rightarrow a * b \in H$

$\forall\ a \in H,\ a^{-1} \in H$

$a \in H,\ a^{-1} \in H$

$a * a^{-1} = e \in H$

$a, b \in H$

$\Rightarrow a * b^{-1} \in H$

Try

(4) $G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$

To prove G is a group under matrix multiplication.

$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ $C = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$

$D = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$

$B \cdot B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$

$BC = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = D$

matrix mult	A	B	C	D
A	A	B	C	D
B	B	I	D	C
C	C	D	A	B
D	D	C	B	A

e, a, b, c

$a^2 = e = b^2 = c^2$

$ab = ba = c$

$bc = cb = a$

$ac = ca = b$

$$C \times C = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$A \times A = A$, $B \times B = A$, $C \times C = A$, $D \times D = A$

$B \times C = C \times B = D$, $C \times D = D \times C = B$

$B \times D = D \times B = C$

I

thus G is closed. Identity is A.

Inverses of B, C, D are

All elements of G are self inverses. Matrix multiplication is always associative.

Also from I, G is abelian

It is nothing but Klein 4 grp.

(3) $(Q^+, *)$ $a * b = \frac{ab}{3}$

Soln Let $a, b \in Q^+$

$a * b = \frac{ab}{3} \in Q^+$. Q^+ is closed under $*$.

Consider $a, b, c \in Q^+$

$$a*(b*c) = a*\left(\frac{bc}{3}\right) = \frac{a \times \frac{bc}{3}}{3} = \frac{abc}{9}$$

$$(a*b)*c = \left(\frac{ab}{3}\right)*c = \frac{\frac{ab}{3} \times c}{3} = \frac{abc}{9}$$

$\therefore a*(b*c) = (a*b)*c \quad \forall a, b, c \in Q^+$

Let $e \in Q^+$ be such that

$$a * e = e * a = a$$

$$a * e = a \Rightarrow \frac{ae}{3} = a \Rightarrow e = 3$$

$$e * a = a \Rightarrow \frac{ea}{3} = a \Rightarrow e = 3$$

Identity element is 3.

For every $a \in Q^+$, to find a^{-1}.

Now assume $a * a^{-1} = a^{-1} * a = 3$

$$a * a^{-1} = 3 \Rightarrow \frac{aa^{-1}}{3} = 3 \Rightarrow a^{-1} = 9/a$$

$$a^{-1} * a = 3 \Rightarrow \frac{a^{-1}a}{3} = 3 \Rightarrow a^{-1} = 9/a$$

$\forall\ a, b \in \mathbb{Q}^+$

$$a * b = \frac{ab}{3} = \frac{ba}{3} = b * a.$$

$\therefore (\mathbb{Q}^+, *)$ is an abelian group.

Example 1.4.1 In the group ({1,−1, i,−i}, ⋅), the subset {1,−1} forms a subgroup because this subset is closed under multiplication

$G = \{1, -1, i, -i\}$ is a group under multiplication.

×	1	−1	i	$-i$
1	1	−1	i	$-i$
−1	−1	1	$-i$	i
i	i	−1	−1	1
$-i$	$-i$	i	1	−1

All the elements in the table are elements of G. Hence G is closed under mult.

'1' is the identity element.

Inverse of i is $-i$ and $-i$ is i

Multiplication is associative.

Also multiplication is commutative.

$\therefore (G, *)$ is an abelian group under multiplication.

Let $H = \{1, -1\} \subset G$. To prove H is a subgroup of G. (ie) to prove $a * b^{-1} \in H \; \forall a, b \in H$

Consider $1, -1 \in H \Rightarrow$. Inverse of -1 is -1. Now $1 \times (-1)^{-1} = 1 \times -1 = -1 \in H$

$\therefore H$ is a subgroup of G under multiplication.

- **<u>Theorem 1</u>:** A subset H of a group G is a subgroup if and only if
- (i) $(a \in H, b \in H) \Rightarrow a * b \in H$ and
  (ii) $a \in H \Rightarrow a' \in H$
- **Proof:**
- Suppose H is a subgroup of G then H must be closed with respect to composition * in G, i.e. $a \in H, b \in H \Rightarrow a * b \in H$.
  Let $a \in H$ and a' be the inverse of a in G. Then the inverse of a in H is also a'. As H itself is a group, each element of H will possess inverse in it, i.e. $a \in H \Rightarrow a' \in H$. Thus the condition is necessary. Now let us examine the sufficiency of the condition.

- **(i) Closure Axiom.** $a \in H, b \in H \Rightarrow a * b \in H$. Hence closure axiom is satisfied with respect to the operation *.
  (ii) Associative Axiom. Since the elements of *H* are also the elements of *G*, the composition is associative in *H* also.
  (iii) **Existence of Identity.** The identity of the subgroup is the same as the identity of the group because, $a \in H, a' \in H \Rightarrow a * a' \in H \Rightarrow e \in H$. The identity *e* is an element of *H*.
  (iv) Existence of Inverse. Since $a \in H \Rightarrow a' \in H$, $\forall a \in H$. Therefore each element of *H* possesses inverse.
  The *H* itself is a group for the composition * in *G*. Hence *H* is a subgroup.

Theorem 2: A necessary and sufficient condition for a non-empty subset H of a group G to be a subgroup is that $a \in H, b \in H \Rightarrow a * b' \in H$ where b' is the inverse of b in G.

- **Proof:** Necessary condition
- Suppose H is a subgroup of G and let $a \in H, b \in H$. Now each element of H must possess inverse because H itself is a group.
- $b \in H \Rightarrow b' \in H$
- Also H is closed under the composition * in G. Therefore
- $a \in H, b' \in H \Rightarrow a * b' \in H$

Sufficient condition

- It is given that $a \in H, b' \in H \Rightarrow a * b' \in H$ then we have to prove that that H is a subgroup
- **(i) Closure Property.** Let $a, b \in H$ then $b \in H \Rightarrow b' \in H$ (as shown above).
- Therefore by the given condition
- $a \in H, b' \in H \Rightarrow a * (b')' \in H \Rightarrow a * b \in H$
- Thus H is closed with respect to the composition $*$ in G.
- **(ii) Associative Property.** Since the elements of H are also the elements of G, the composition is associative in H.

- **(iii) Existence of Identity.** Since

- $a \in H, a' \in H \Rightarrow a * a' \in H \Rightarrow e \in H$
-
  (iv) Existence of Inverse. Let $a \in H$ then

- $e \in H, a \in H \Rightarrow e * a' \in H \Rightarrow a' \in H$

Then each element of H possesses inverse.
Hence H itself is a group for the composition $\circ$ in group G.

- Defn: The order of an element a in G is the least positive integer m such that $a^m=e$, e is the identity of G.

Definition. The *order* of a group $(G,*)$, is the number of elements in the set G, denoted $|G|$ (which may be infinite). Note that $|G| \geq 1$, since every group contains at least one element (the identity element).

1) Consider $G = \{1, -1, i, -i\}$. Find the order of all the elements in G.

Solution Now $1^1 = 1 \Rightarrow o(1) = 1$

$(-1)^2 = 1 \Rightarrow o(-1) = 2$

$i^1 = 1$, $i^2 = -1$, $i^3 = -i$, $i^4 = 1 \Rightarrow o(i) = 4$

$(-i)^1 = -i$, $(-i)^2 = -1$, $(-i)^3 = -i^3 = i$, $(-i)^4 = i^4 = 1$

$\Rightarrow o(-i) = 4$

(2) Find the order of every element in $(Z_5, +_5)$.

Sol: 0 is the identity element.

$Z_5 = \{0, 1, 2, 3, 4\}$

$ord(0) = 1$, $1 +_5 1 +_5 1 +_5 1 +_5 1 = 0$

$\Rightarrow ord(1) = 5$

$2 +_5 2 +_5 2 +_5 2 +_5 2 = 0 \Rightarrow ord(2) = 5$

$3 +_5 3 +_5 3 +_5 3 +_5 3 = 0 \Rightarrow ord(3) = 5$

$4 +_5 4 +_5 4 +_5 4 +_5 4 = 0 \Rightarrow ord(4) = 5$

(3) Find the order of every element in $(Z_6, +_6)$.

Soln: $Z_6 = \{0, 1, 2, 3, 4, 5\}$

$1 +_6 1 +_6 1 +_6 1 +_6 1 +_6 1 = 0 \Rightarrow o(1) = 6$

$2 +_6 2 +_6 2 = 0 \Rightarrow o(2) = 3$

$4 +_6 4 +_6 4 = 0 \Rightarrow o(4) = 3$

$5 +_6 5 +_6 5 +_6 5 +_6 5 +_6 5 = 0 \Rightarrow o(5) = 6$

Cyclic Groups

- A group G is said to be cyclic if

$$G = < a > = \{a^k : k \in Z\}$$

Proposition 192 *Get G be a group and $a \in G$. Let m and n be integers. The following is true:*

1. $a^m a^n = a^{m+n}$
2. $(a^m)^n = a^{mn}$
3. $(a^n)^{-1} = a^{-n} = (a^{-1})^n$
4. $a^0 = e$

Example 193 *$\mathbb{Z}$ is cyclic since $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$*

Example 194 *$\mathbb{Z}_n$ with addition $\bmod n$ is a cyclic group, 1 and $-1 = n-1$ are generators.*

Cyclic group

$a, a*a, a*a*a, a*a*a*a, \ldots$

$G = \{1, -1, i, -i\}$ $\quad i = \sqrt{-1}$

$= \{i, i \cdot i, i \cdot i \cdot i, i \cdot i \cdot i \cdot i\}$

$= \{i, -1, -i, 1\}$

$G = \{-i, -i * -i, -i \cdot -i \cdot -i, -i \cdot -i \cdot -i \cdot -i\}$

$= \{-i, -1, i, 1\}$

$|G| = n$

$G = \{a, a*a, a*a*a, a*a*a*a, \ldots, a*a*a*\cdots*a = e\}$

$(Z_4, +_4)$ is a group

$Z_4 = \{0, 1, 2, 3\}$

~~$1 +_4 1$~~; $1 +_4 1 = 2$, $1 +_4 1 +_4 1 = 3$,

$1 +_4 1 +_4 1 +_4 1 = 0$

3, $3 +_4 3 = 2$, $3 +_4 3 +_4 3 = 2 +_4 3 = 1$

$3 +_4 3 +_4 3 +_4 3 = 1 +_4 3 = 0$

1 and 3 are generators

$2,\ 2 +_4 2 = 0,\ 0 +_4 2 +_4 2 +_4 2$

$= 0 +_4 2 = 2$

2 is not a generator

1 is a generator

$2 = 1 +_4 1$

$n = 4$

$\gcd(2,4) \neq 1$

Whenever a is a generator, $a * a * \cdots * a$ (m times)

is also a generator iff $\gcd(m,n) = 1$

where $|G| = n$

$G = \{1, -1, i, -i\}$ $\quad |G| = 4$

i is a generator.

$i \cdot i = i^2$ But $\gcd(2,4) \neq 1$

$i \cdot i \cdot i = i^3 = -i$ $\gcd(3,4) = 1$

$(Z_5, +_5)$ $\quad Z_5 = \{0, 1, 2, 3, 4\}$

$1, \; 1 +_5 1 = 2, \; (1 +_5 1) +_5 1 = 3, \; 1 +_5 1 +_5 1 +_5 1 = 4$

$1 +_5 1 +_5 1 +_5 1 +_5 1 = 0$

'1' is a generator

1, 2, 3, 4 all are generators because

$$\gcd(1,5) = \gcd(2,5) = \gcd(3,5) = \gcd(4,5) = 1$$

$(Z_6, +_6)$ $\quad Z_6 = \{0, 1, 2, 3, 4, 5\}$

1 and 5 are generators. Since

$\gcd(1,6) = \gcd(5,6) = 1$

Infinite cyclic group G/g

$(Z, +)$ is cyclic $\{e, g, g^2, g^3, \ldots, g^{n-1}\}$

$\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, \ldots$

$\{\infty, \ldots, 10, 9, 8, \ldots 0, \}$

Eg $(Z_{15}, +_{15})$

$1, 2, 4, 7, 8, 11, 13, 14$ $\quad (1 +_{15} \cdots)$

Klein 4 group

$|G| = n \geq 5$

$|G| = n = 4$

$S_3 = \{ I, (12), (13), (23), (123), (132) \}$

(1) All groups of prime order are cyclic

(2) Groups of order ≤ 4 is always abelian

① Find all generators of Z_6, Z_8, Z_{20}

Solution Z_6 Generators are 1, 5.

Z_8 Generators 1, 3, 5, 7

Z_{20} Generators 1, 3, 7, 9, 11, 13, 17, 19

② $O(a) = 60$. Find the order of a^{24}.

Soln. $O(a) = 60 \Rightarrow a^{60} = e$

$(a^{24})^m = e$. To find m

$m=1$	$a^{24} \neq e$
$m=2$	$a^{48} \neq e$
$m=3$	$a^{72} \neq 0$
$m=5$	$a^{120} = e$

$5 \overline{)15, 20}$
$3, 4$

(3) If $O(a) = 15$, find $O(a^{20})$

Soln $a^{15} = e$ (Given)

To find m such that $(a^{15})^m = e$

$m=1$ $(a^{20})^1 \neq e$ | $m=2$ $(a^{20})^2 \neq e$

$m=3$ $(a^{20})^3 = a^{60} = (a^{15})^4 = e^4 = e$

$\therefore O(a^{20}) = 3$

Theorem 197 *Every cyclic group is Abelian*

Proof. *The elements of cyclic groups are of the form a^i. Commutativity amounts to proving that $a^i a^j = a^j a^i$.*

$$\begin{aligned} a^i a^j &= a^{i+j} \\ &= a^{j+i} \text{ addition of integers is commutative} \\ &= a^j a^i \end{aligned}$$

■

TRY

- Find all generators of Z_6,Z_8 and Z_{20}.
- If order(a)=60, what is the order of a^{24}?
- Note: For infinite cyclic groups, only two generators are possible (ie) if a is a generator , then a^{-1} is a generator.

(1) Generators of Z_{20}

$Z_{20} = \{0, 1, 2, 3, \ldots, 19\}$

1, 3, 7, 9, 11, 13, 17, 19 are generators of Z_{20}

Examples.

1. If $(G, *)$ is a group with identity element e_G, then G and $\{e_G\}$ are subgroups of $(G, *)$. The criteria of the subgroup test are easily checked.

2. Let us check the criteria of the subgroup test in the case of the subgroup $n\mathbb{Z}$ of $(\mathbb{Z}, +)$, where n is a positive integer. Firstly, $n\mathbb{Z}$ is closed with respect to addition, since $nk + n\ell = n(k+\ell) \in n\mathbb{Z}$. Secondly, the identity element, $0 = n \cdot 0$ belongs to $n\mathbb{Z}$. Finally, the inverse of nk in $(\mathbb{Z}, +)$ is $-nk = n(-k) \in n\mathbb{Z}$.

3. Consider the cyclic group $(\mathbb{Z}_3, +)$. We already know that there are at least two subgroups of this group, namely $\mathbb{Z}_3$ itself and $\{0\}$. If $H \neq \{0\}$ is a subgroup, then $0 \in H$, so H must also contain an element other than 0, ie 1 or 2. But if $1 \in H$ then $2 = 1 + 1 \in H$ since H is closed. Similarly if $2 \in H$ then $1 = 2 + 2 \in H$. Thus $H = \mathbb{Z}_3$. Thus $\mathbb{Z}_3$ has precisely two subgroups, namely $\mathbb{Z}_3$ itself and the trivial subgroup $\{0\}$.

4. Now consider the cyclic group $(\mathbb{Z}_4, +)$. As in the previous example, if H is a subgroup and $1 \in H$, then $2 = 1 + 1 \in H$ and $3 = 2 + 1 \in H$, so $H = \mathbb{Z}_4$. Similarly, if $3 \in H$ then $H = \mathbb{Z}_4$ since $2 = 3 + 3$ and $1 = 2 + 3$. Thus, if $H \neq \mathbb{Z}_4$ is a subgroup of $(\mathbb{Z}_4, +)$, then $\{0\} \subset H \subset \{0, 2\}$, so H is either equal to the trivial

subgroup $\{0\}$ or to $\{0,2\}$. It is easy to check that $\{0,2\}$ satisfies the criteria of the subgroup test, so it is also a subgroup of $(\mathbb{Z}_4,+)$. Thus $(\mathbb{Z}_4,+)$ has precisely three subgroups: $\{0\}$, $\{0,2\}$, and $\mathbb{Z}_4$.

5. Let $i \in \{1,2,\ldots,n\}$, and define H_i to be the subset $H_i = \{\sigma \in S_n;\ \sigma(i) = i\}$ of S_n. Then H_i is a subgroup. To see this, let us check the criteria from the subgroup test

   - H_i is closed: if $\sigma, \tau \in H_i$ then $(\sigma \circ \tau)(i) = \sigma(\tau(i)) = \sigma(i) = i$, so $\sigma \circ \tau \in H_i$.
   - The identity element id belongs to H_i: $id(i) = i$.
   - if $\sigma \in H_i$, then $\sigma^{-1} \in H_i$. Suppose that $\sigma^{-1}(i) = j$. Then $\sigma(j) = i = \sigma(i)$. Since σ is injective, $i = j$. Hence $\sigma^{-1}(i) = i$, in other words $\sigma^{-1} \in H_i$.

Examples.

1. $|\mathbb{Z}_m| = m$ for any positive integer m.

2. In $(\mathbb{Z}_4, +)$ the orders of the elements are as follows: $|0| = 1$ since 0 is the identity element; $|2| = 2$, since $2 \neq 0$ but $2 + 2 = 0$; $|1| = 4$ since $1 + 1 + 1 + 1 = 0$ but $1 \neq 0, 1 + 1 \neq 0, 1 + 1 + 1 \neq 0$; and $|3| = 4$ for similar reasons.

3. $|GL_2(\mathbb{R})| = \infty$, since there are infinitely many invertible 2×2 matrices with real entries. In $GL_2(\mathbb{R})$ the order of $A = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ is 6, since $A^6 = I_2$ but $A^k \neq I_2$ for $1 \leq k \leq 5$. (Exercise: try this and see.)

COSETS

Definition 1.1. Let G be a group and H be a subgroup. For $g \in G$, the sets

$$gH = \{gh : h \in H\}, \quad Hg = \{hg : h \in H\}$$

are called, respectively, a *left H-coset* and a *right H-coset*.

The best way to think about cosets is that they are *shifted subgroups*, or *translated subgroups*.

Cosets

$(G, *)$ is a group and $(H, *)$ is a subgroup of $(G, *)$.

Left coset

$\forall\, g \in G$

$$g * H = \{ g * h \mid h \in H \}$$

Example

Let $G = \{1, -1, i, -i\}$. G is a group under multiplication and $H = \{1, -1\}$ is a subgroup of G.

$$1 * H = 1 \cdot H = 1 \cdot \{1, -1\} = \{1, -1\} = H$$

$$-1 * H = -1 \cdot H = -1 \{1, -1\} = \{-1, 1\} = H$$

$i * H = i\{1, -1\} = \{i, -i\}$

$-i * H = -i\{1, -1\} = \{-i, i\}$

$H = 1 \cdot H = -1 \cdot H$

$i \cdot H = -i\, H$

There are 2 distinct left cosets.

Right cosets $H * g = \{h * g \mid h \in H\}$

$H * 1 = H \cdot 1 = \{1, -1\} \cdot 1 = \{1, -1\} = H$

$H * -1 = H \cdot (-1) = \{1, -1\}(-1) = \{-1, 1\} = H$

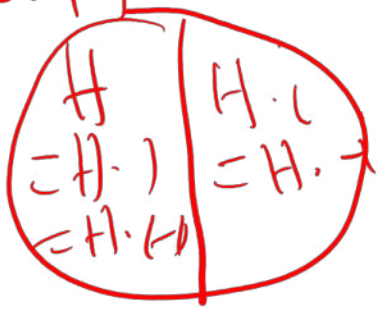
$H * i = H \cdot i = \{1, -1\} \cdot i = \{i, -i\}$

$H * -i = H \cdot -i = \{1, -1\}(-i) = \{-i, i\}$

$H = H \cdot 1 = H \cdot (-1)$

$H \cdot i = H \cdot (-i)$

There are 2 different right cosets



Find the left and right cosets of S_3

$G = S_3 = \{I, (12), (13), (23), (123), (132)\}$

$H = \{I, (123), (132)\}$

Left cosets

$I * H = IH = I\{I, (123), (132)\}$

$= \{I \cdot I, I(123), I(132)\}$

$= \{I, (123), (132)\}$

$(12) * H = \{(12)I, (12)(123), (12)(132)\}$

$= \{(12), (23), (13)\}$

$G = S_3 = \{I, (12), (13), (23), (123), (132)\}$

$H = \{I, (123), (132)\}$

Left cosets of H in G

$I\,H = I\{I, (123), (132)\} = \{I, (123), (132)\}$

$= H$

$(12)\,H = (12)\{I, (123), (132)\}$

$= \{(12)(23), (13)\}$

$(13)\,H = (13)\{I, (123), (132)\}$

$= \{(13), (12), (23)$

$(23)H = (23)\{I, (123), (132)\}$

$= \{(23), (13), (12)\}$

$(123)H = (123)\{I, (123), (132)\}$

$= \{(123), (132), I\}$

$(132)H = (132)\{I, (123), (132)\}$

$= \{(132), I, (123)\}$

$(12)H = (13)H = (23)H$

$H = IH = (123)H = (132)H$

There are 2 different left cosets

Right cosets

$H \cdot I = \{I, (123), (132)\} I = H$

$H \cdot (12) = \{I, (123), (132)\}(12) = \{(12), (13), (23)\}$

$H \cdot (13) = \{(12), (13), (23)\}$

$H \cdot (23) = \{(12), (13), (23)\}$

$H(123) = \{I, (123), (132)\}(123)$

$= H$

$H(132) = H$

$\therefore H = HI = H(123) = H(132)$

$H(12) = H(13) = H(23)$

$$(13)*H = \{(13)I,\ (13)(123),(13)(132)\}$$

$$= \{(13),\ (12),\ (23)\}.$$

$$(23)*H = \{(23)I,(23)(123),\ (23)(132)\}$$

$$= \{(23),\ (13),\ (12)\}$$

$$(123)*H = \{(123)I,\ (123)(123),\ (123)(132)\}$$

$$= \{(123),\ (132),\ I\}$$

$$(132)*H = \{(132)I,\ (132)(123),\ (132)(132)\}$$

$$= \{(132),\ I,\ (123)\}$$

$I H = (123) H = (132) H = H$

$(12) H = (13) H = (23) H$

There are 2 distinct cosets.

Right cosets $H \cdot I = H$

$H \cdot (123) = \{I, (123), (132)\} \cdot (123)$

$= H$

$H \cdot (132) = \{I, (123), (132)\} \cdot (132)$

$= H$

$H \cdot (12) = \{(12), (13) (23)\} = H \cdot (13)$

$= H \cdot (23)$

$$G = S_3 = \{I, (12), (13), (23), (123), (132)\}$$

$$H = \{I, (12)\}$$

Example 1.2. In the additive group $\mathbf{Z}$, with subgroup $m\mathbf{Z}$, the $m\mathbf{Z}$-coset of a is $a + m\mathbf{Z}$. This is just a congruence class modulo m.

Example 1.3. In the group $\mathbf{R}^\times$, with subgroup $H = \{\pm 1\}$, the H-coset of x is $xH = \{x, -x\}$. This is "x up to sign."

Example 1.4. When $G = S_3$, and $H = \{(1), (12)\}$, the table below lists the left H-cosets and right H-cosets of every element of the group. Compute a few of them for non-identity elements to satisfy yourself that you understand how they are found.

g	gH	Hg
(1)	$\{(1), (12)\}$	$\{(1), (12)\}$
(12)	$\{(1), (12)\}$	$\{(1), (12)\}$
(13)	$\{(13), (123)\}$	$\{(13), (132)\}$
(23)	$\{(23), (132)\}$	$\{(23), (123)\}$
(123)	$\{(13), (123)\}$	$\{(23), (123)\}$
(132)	$\{(23), (132)\}$	$\{(13), (132)\}$

Properties of Cosets:

- Let H be a subgroup of G, and a,b in G.
- 1. a belongs to aH
- 2. aH = H iff a belongs to H
- 3. aH = bH iff a belongs to bH
- 4. aH and bH are either equal or disjoint
- 5. aH = bH iff $a^{-1}b$ belongs to H
- 6. |aH| = |bH|
- 7. aH = Ha iff H = aHa^{-1}
- 8. aH ≤ G iff a belongs to H

$aH = Ha$ iff $H = aHa^{-1}$

- Proof: $aH = Ha$

  <=> each $ah = h'a$ for some h' in H

  <=> $aha^{-1} = h'$ for some h' in H

  <=> $H = aHa^{-1}$.

□

EXAMPLES

- 1. **If G is the additive group of integers and H is the subgroup of G obtained by multiplying each element of G by 3, find the distinct right cosets of H in G.**

- **Soln:**

- **G={…..,-3,-2,-1,0,1,2,3,….}**
- **H={…..,-9,-6,-3,0,3,6,9,….}**
- **H+0={….,-9,-6,-3,0,3,6,9,…}**
- **H+1={…,-8,-5,-2,1,4,7,10,…}**
- **H+2={….,-7,-4,-1,2,5,8,11,….}**
- **H+3=H**
- **H+4=H+1, H+5=H+2, H+6=H, H+(-1)=H+2,**
- **H+(-2)=H+1, H+(-3)=H so on.**

$(\mathbb{Z}, +)$

$G = \mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

$H = 3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$

$3\mathbb{Z} + 0 = H$

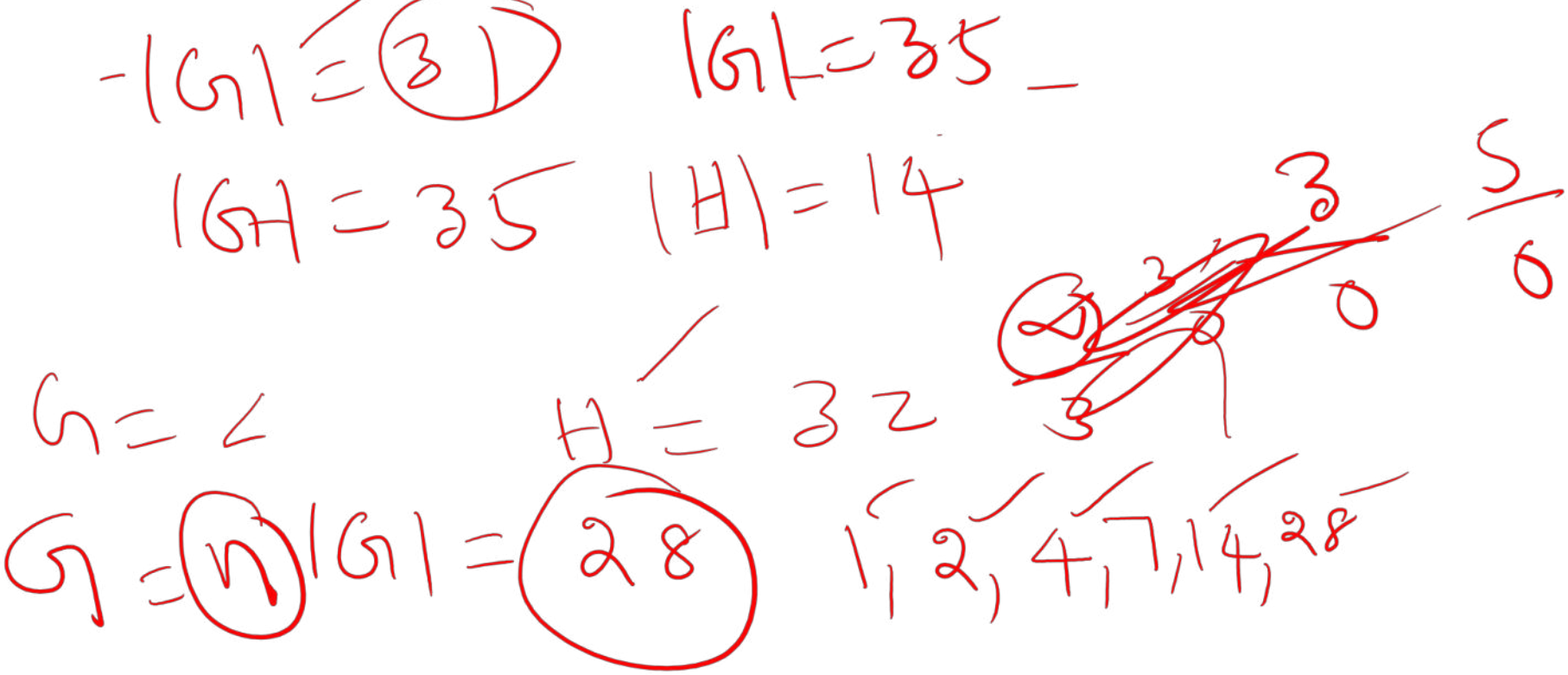
$3\mathbb{Z} + 1 = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$

$3\mathbb{Z} + 2 = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$

$3\mathbb{Z} + 3 = \{\ldots, -6, -3, 0, 3, 6, \ldots\} = 3\mathbb{Z}$

LAGRANGE'S THEOREM

- Statement: The order of a subgroup of a finite group is a divisor of the order of the group.



Example 17.1

If $|G| = 14$ then the only possible orders for a subgroup are 1, 2, 7, and 14.∎

Definition 17.1

The number of different right cosets of H in G is called the **index** of H in G and is denoted by $[G : H]$.

It follows from the above definition and the proof of Lagrange's theorem that

$$|G| = [G : H]|H|.$$

Example 17.2

Since $|S_3| = 3! = 6$ and $|(12)| = |< (12) >| = 2$ then $[S_3, < (12) >] = \frac{6}{2} = 3$.∎

GROUP HOMOMORPHISM

- Defn : If (G,*) and (G',#) are two groups, then a mapping $f : G \to G'$ is called a group homomorphism, if for any a,b in G
- f(a*b)=f(a)#f(b)
- Theorem:
- If $f : G \to G'$ is a group homomorphism from (G,*) to (G',#), then
- (i)f(e)=e' (ii)$f(a^{-1})=[f(a)]^{-1}$

Group Homomorphism

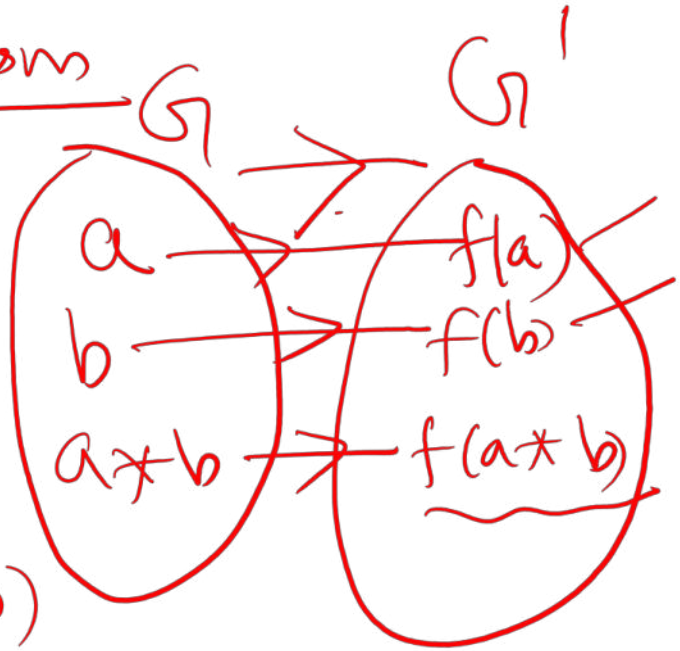
$(G, *)$ $(G', \#)$

$f : G \to G'$

$f(a * b) = f(a) \# f(b)$

$f(a *_1 b) = f(a) *_2 f(b)$

f is a homomorphism



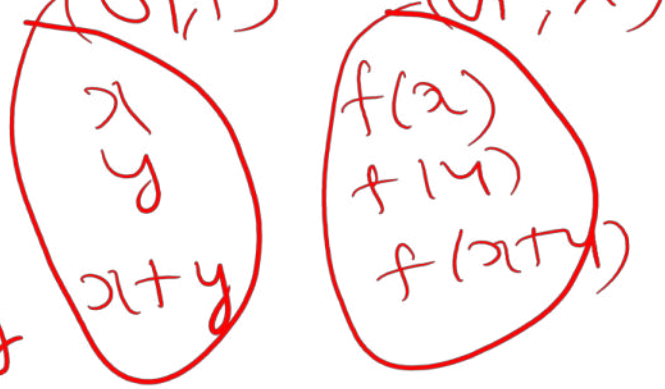
(1) $G = \mathbb{R}$, $(\mathbb{R}, +)$ is a group

$G' = \mathbb{R}^+$ $(\mathbb{R}^+, \times)$ is a group

$f : G \to G'$ as $f(x) = 2^x$, $x \in \mathbb{R}$.

To prove $\forall x, y \in G$,

$$f(x+y) = f(x) \times f(y)$$

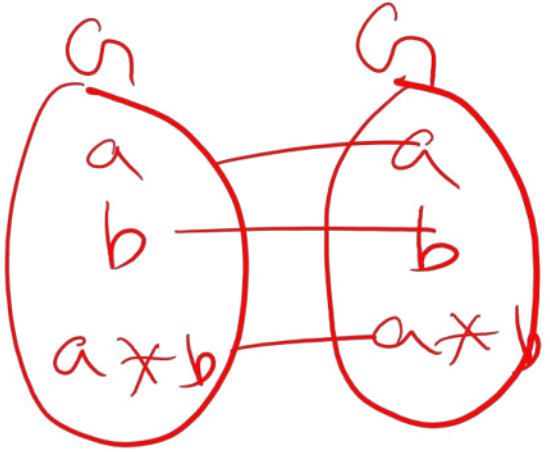


$$f(x+y) = 2^{x+y} = 2^x \times 2^y$$

$$= f(x) \times f(y)$$

$\therefore$ f is a homomorphism

② $(G, *)$ is a group



$f(a) = a$

To prove

$f(a*b) = f(a) * f(b)$

Now $f(a*b) = a*b = f(a) * f(b)$

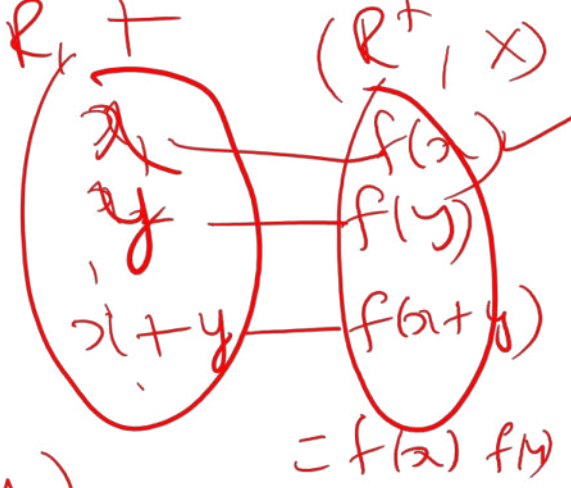
$\therefore$ f is a homomorphism

EXAMPLE

- If G is a group of real numbers under addition and G' is the group of positive real numbers under multiplication, show that the mapping defined by $f(x)=2^x$ is a homomorphism.
- If G is a group with identity e, show that the mapping $f:G\rightarrow G$ defined by $f(a)=a$, for every a in G is a homomorphism.

(1) $f: (\mathbb{R}, +) \to (\mathbb{R}^+, \times)$

$f(x) = 2^x$



To prove

$f(x+y) = f(x) \times f(y)$

$f(x+y) = 2^{x+y} = 2^x \, 2^y = f(x) f(y)$

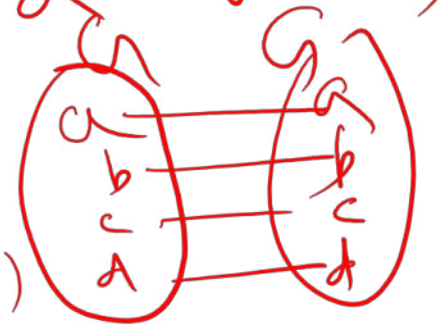
Hence f is a homomorphism

(2) $f: G \to G$ where $(G, *)$ is a group by $f(a) = a \quad \forall a \in G$

To prove: $f(a*b) = a*b$

$= f(a) * f(b)$

$\therefore f$ is a homomorphism



$(Z_6, +_6)$ $\cdot$ $Z_6 = \{0, 1, 2, 3, 4, 5\} = G$

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

$0 +_6 H = H$, $1 +_6 H = \{1, 3, 5\}$

$2 +_6 H = H$

$3 +_6 H = \{1, 3, 5\}$

$4 +_6 H = H$

$5 +_6 H = \{1, 3, 5\}$

$0 +_6 H = 2 +_6 H = 4 +_6 H$

and

$1 +_6 H = 3 +_6 H = 5 +_6 H$