- g is a generator in S
- $g^n = \underbrace{g \circ g \circ \cdots \circ g}_{n \text{ times}}$
- $\circ \leftarrow +$, $g^n = g+g+\cdots+g$ (n times)
- $\circ \leftarrow \times$, $g^n = g \times g \times \cdots \times g$ (n times)

$\langle M, \circ \rangle$, $[M, \circ]$, $(M, \circ)$

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

Composition Table

$\times$	-1	1	i	$-i$
-1	1	-1	$-i$	i
1	-1	1	i	$-i$
i	$-i$	i	-1	1
$-i$	i	$-i$	1	-1

$i^2 = -1$

$-i^2 = 1$

1) closed under $\times$
2) Associative under $\times$

$$\left.\begin{array}{l} i \times (-i \times 1) = i \times (-i) = 1 \\ (i \times (-i)) \times 1 = 1 \times 1 = 1 \end{array}\right\}$$

3) Identity: $1 \in S$ is the identity.

4) Inverse:

ω	ω^{-1}
1	1
-1	-1
i	$-i$
$-i$	i

$\therefore \langle S, \times \rangle$ is a group.

PART 2.

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

$\therefore S = \{-1, 1, i, -i\} = \{i^1, i^2, i^3, i^4\}$

$\Rightarrow i \in S$ is a generator in S

2) $(-i)^1 = -i$

$(-i)^2 = -1$ $\quad S = \{-1, 1, i, -i\}$

$(-i)^3 = i$ $\quad = \{(-i)^1, (-i)^2, (-i)^3, (-i)^4\}$

$(-i)^4 = 1$ $\Rightarrow -i \in S$ is another generator in S.

• Problem: Given $[S, \cdot]$ is a semigroup

Given $\forall a, b \in S$, $\exists x, y \in S$ s.t.

$x \cdot a = b$

$a \cdot y = b$

Required to prove (RTP): $\langle S, \cdot \rangle$ is a group.

ie, RTP: (i) closure holds, since $[S, \cdot]$ is a semigroup.

(ii) associativity holds, since $[S, \cdot]$ is a semigroup.

* (iii) RTP: $\forall x \in S$, $e \cdot x = x \cdot e = x$, ie, $e \in S$ is the identity in S

and

* (iv) RTP: $\forall x \in S$, $\exists x^{-1} \in S$ s.t. $x^{-1} \cdot x = x \cdot x^{-1} = e$, ie, $x^{-1} \in S$ is the inverse of x in S.

(iii) Let $a = b$. Then $\forall a \in S$, $\exists x, y \in S$ s.t. $x \cdot a = a$ and $a \cdot y = a$ ... (1)

~~Let~~ $c \in S$. Then, $\exists\, x_1, y_1 \in S$ s.t.

$x_1 \cdot a = c$ and $a \cdot y_1 = c$ ... (2)

Now, $x \cdot c = x \cdot (a \cdot y_1)$

$= (x \cdot a) \cdot y_1$, by associative

$= a \cdot y_1$

$= c$

$\Rightarrow x \in S$ is the left identity.

Similarly, $c \cdot y = (x_1 \cdot a) \cdot y$

$= x_1 \cdot (a \cdot y)$

$= x_1 \cdot a$

$= c$

$\Rightarrow y \in S$ is the right identity.

[Uniqueness] R.T.P: $x = y$.

Now, $x = x \cdot y$ [because ~~x~~ y is the right identity]

$= y$ [" x is the left identity]

$\therefore \forall x \in S, \exists\, e \in S$ s.t. $x \cdot e = e \cdot x = x$.

(iv) ~~Let~~ $b = e$

$\therefore \forall a \in S, \exists\, x \in S$ s.t. $x \cdot a = e$ and $a \cdot y = e$.

Now, $x = x \cdot e$

$\Rightarrow x = x \cdot (a \cdot y) = (x \cdot a) \cdot y = e \cdot y = y$

Hence, $x \cdot a = e$ and $a \cdot x = e$

$\Rightarrow x \in S$ is the inverse of $a \in S$.

$\therefore [S, \cdot]$ is a group.