if $n > 1$ then $U(n)$ is group with respect to multiplication modulo n.

Proof $\quad U(n) = \{x \in \mathbb{N} : 1 \leq x \leq n$ and $g.c.d(x, n) = 1\}$
$\forall\ n > 1$.

(i) let $a \in U(n)$ then $1 \leq a \leq n$ and $g.c.d(a, n) = 1$

$b \in U(n)$ then $1 \leq b \leq n$ and $g.c.d(b, n) = 1$

Now since $(a, n) = 1$ and $g.c.d(b, n) = 1$

$\Rightarrow g.c.d(ab, n) = 1$

$\Rightarrow a \cdot b \in U(n)$ under multiplication modulo n.

$\Rightarrow$ Cloure property hold.

(ii) let $a, b, c \in U(n)$

then $1 \leq a \leq n$, and $g.c.d(a, n) = 1$

$1 \leq b \leq n$ and $g.c.d(b, n) = 1$

$1 \leq c \leq n$ and $g.c.d(c, n) = 1$

$a \cdot (b \cdot c) = (a\, b) \cdot c \quad \forall\ a, b, c \in U(n)$

hence Associative property hold.

(iii) since $1 < n$ and $g.c.d(1, n) = 1$ then $1 \in U(n)$

such that $a \cdot 1 = a \quad \forall\ a \in U(n)$.

$\Rightarrow \exists$ identity 1.

(iv) Let $a \in U(n)$ then $g.c.d(a, n) = 1$

$\Rightarrow ax \equiv 1 \pmod{n}$ has solⁿ then $x = a^{-1}$ exist w.r.to modulo n.

then $x = a^{-1} \in U(n)$ s.t. $a a^{-1} = a^{-1} a = 1$

i.e. $\exists$ inverse $\forall\, a \in U(n)$

$\Rightarrow$ $U(n)$ is group w.r.to multiplicatio modulo n.

Ex 1) To show $U(7)$ is group.

$U(7) = \{x \in \mathbb{N} : 1 \le x \le n$ and g.c.d $(x, n) = 1\}$

$U(7) = \{1, 2, 3, 4, 5, 6\}$.

(1) let $a, b \in U(7)$ s.t. $a \cdot b \in U(7)$ under multiplication moduloo n.

for eg:- $3 \in U(7)$, $6 \in U(7)$

$6 \cdot 3 = 18 = 4 \in U(7)$

$7 \,)\, 18 \,(\, 2$
$\quad 14$
$\quad \overline{\ \ 4}$

again $5 \in U(7)$, $2 \in U(7)$

$5 \cdot 2 = 10 = 3 \in U(7)$

$7 \,)\, 10 \,(\, 1$
$\quad 7$
$\quad \overline{\ 3}$

$\Rightarrow$ closure property hold.

(ii) let $a, b, c \in U(7)$ s.t.

$(a \cdot b) \cdot c = a \cdot (b \cdot c) \in U(7)$, $\forall\, a, b, c \in U(7)$

under multiplication modulo n.

for eg:- $3, 4, 5 \in U(7)$

$(3 \cdot 4) \cdot 5 = 60 = 4 \in U(7)$

$3 \cdot (4 \cdot 5) = 60 = 4 \in U(7)$ Associative property hold.

(iii) $\exists \; 1 \in U(7)$ s.t.

$1 \cdot a = a \cdot 1 = a \quad \forall \; a \in U(7)$ under multiplication modulo 7.

hence $\exists$ identity $1 \in U(7)$.

(iv) let $a \in U(7)$ then $g.c.d\,(a, 7) = 1$

$ax \equiv 1 \pmod 7$ has sol^n then $x = a^{-1}$ exist w.r.to. modulo n.

then $x = a^{-1} \in U(7)$ s.t. $aa^{-1} = a^{-1}a = 1$

ie. $\exists$ inverse $\forall \; a \in U(7)$.

for eg:- $6 \in U(7)$, $g.c.d\,(6, 7) = 1$

$6x \equiv \pmod 7$

$x = 6^{-1} = 6$

i.e. $6 \cdot 6^{-1} = 6 \cdot 6 = 36 = 1 \pmod 7$.

now, $5 \in U(7)$, $g.c.d\,(5, 7) = 1$

$5x \equiv 1 \pmod 7$

$x \equiv 5^{-1} = 3$

$5 \cdot 5^{-1} = 5 \cdot 3 = 15 = 1 \pmod 7$

$\Rightarrow$ $U(7)$ is a group under multiplication modulo 7.

Q To show $U(8)$ is a group under multiplication modulo 8

$U(8) = \{1, 3, 5, 7\}$ and Find the inverse of each element of $U(8)$.

Q. $G = U(12) = \{1, 5, 7, 11\}$. To show $U(12)$ is a group under multiplication modulo 12 and Find inverse of each element.

Q. $U(10) = \{1, 3, 7, 9\}$. To show show $U(10)$ is a group under multiplication modulo 10. and Find inverse of each element.

Quaternion Group

Show that Quaternion group Q_4 Form a group under multiplication.

$$Q_4 = \{-1, 1, i, -i, -j, j, k, -k\}$$

s.t. $i^2 = j^2 = k^2 = -1$

$i \cdot j = -j \cdot i = k$

$jk = -kj = i$

$ki = -ik = j$.

(i) $\forall a \in Q_4, \forall b \in Q_4$ s.t. $a \cdot b \in Q_4$ [Closure property]

(ii) $a \cdot (b \cdot c) = abc = (a \cdot b) \cdot c$ $\forall a, b, c \in Q_4$. [Associative Property]

(iii) $1 \in Q_4$ s.t. $a \cdot 1 = a$ $\forall a \in Q_4$. [existence of identity]

(iv) Inverse of each element of Q_4.

$1^{-1} = 1$ [i.e. $1 \cdot 1 = 1$]

$-1^{-1} = -1$ [i.e $(-1) \cdot (-1) = 1$]

$i^{-1} = -i$ [$i \cdot (-i) = 1$]

$-i^{-1} = i$ (i.e. $(-i) \cdot i = 1$)

$j^{-1} = -j$ (i.e. $j \cdot (-j) = 1$)

$k^{-1} = -k$ (i.e. $k(-k) = 1$)

$-k^{-1} = k$ (i.e. $(-k) \cdot k = 1$)

$\Rightarrow Q_4$ is a group.

Q. Show that K_4 (Kelin's group) under multiplication.

Proof:- $K_4 = \{e, a, b, ab : a^2 = e, b^2 = e, ab = ba\}$.

$\cdot$	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ba	b	a	e

(i) from Table, $\forall a \in K_4, \forall b \in K_4$ s.t.
$ab \in K_4$ (Closure Property hold)

(ii) $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in K_4$
Associative property hold.

(iii) $e \in K_4$ s.t. $a \cdot e = e \cdot a = a \quad \forall a \in K_4$.

(iv) Inverse of each element of K_4.
$e^{-1} = e$ (i.e. $e \cdot e = e^2 = e$)
$a^{-1} = a$ (i.e. $a \cdot a = e$)
$b^{-1} = b$ (i.e. $b \cdot b = e$)
$(ab)^{-1} = ab$ (i.e. $(ab)(ab) = a(ba)b$
$= a(ab)b = a^2 b^2 = e \cdot e = e$

$\Rightarrow (K_4, \cdot)$ is group