2.2) a)

Closure

$\bar{a} \oplus \bar{b} = \overline{a+b}$

$= \{x \in \mathbb{R} : x - (a+b) = 0 \pmod n\}$

$a+b$ can be written in the form $n.q + r$, $q, r \in \mathbb{Z}$, $0 \le r < n$ ∵ Euclidean division

$\Rightarrow \bar{a} \oplus \bar{b} = \{x \in \mathbb{Z} : x - (n.q + r) = 0 \pmod n\}$

$= \{x \in \mathbb{Z} : x - r = 0 \pmod n\}$

$= \bar{r} \in \mathbb{Z}_n$

$(\mathbb{Z}_n, \oplus)$ is closed.

Associativity

$(\bar{a} \oplus \bar{b}) \oplus \bar{c} = \overline{a+b} \oplus \bar{c}$

$= \overline{(a+b)+c}$

$= \overline{a+b+c}$

$\bar{a} \oplus (\bar{b} \oplus \bar{c}) = \bar{a} \oplus \overline{b+c}$

$= \overline{a + (b+c)}$

$= \overline{a+b+c}$

$\Rightarrow (\bar{a} \oplus \bar{b}) \oplus \bar{c} = \bar{a} \oplus (\bar{b} \oplus \bar{c})$

$(\mathbb{Z}_n, \oplus)$ is associative.

Neutral element

$\bar{a} \oplus \bar{e} = \bar{a}$

$\Rightarrow \overline{a+e} = \bar{a}$

$\Rightarrow \{x \in \mathbb{Z} : x - (a+e) = 0 \pmod n\} = \{x \in \mathbb{Z} : x - a = 0 \pmod n\}$

$\Rightarrow \bar{e} = \bar{0} \in \mathbb{Z}_n$

$\bar{0} \oplus \bar{a} = \overline{0+a}$

$= \bar{a}$

$\Rightarrow (\mathbb{Z}_n, \oplus)$ has neutral element $\bar{0}$.

Inverse element

$\bar{a} \oplus \overline{a^{-1}} = \bar{e}$

$\Rightarrow \overline{a + a^{-1}} = \bar{0}$

$\Rightarrow \{x \in \mathbb{Z} : x - (a+a^{-1}) = 0 \pmod n\} = \{x \in \mathbb{Z} : x = 0 \pmod n\}$

$\Rightarrow a + a^{-1}$ is a multiple of n.

Let $a + a^{-1} = n.k$, $k \in \mathbb{Z}$

$a = 0 \Rightarrow a^{-1} = n.k$

$\Rightarrow k = 0$, $\overline{a^{-1}} = \bar{0} \in \mathbb{Z}_n$

$0 < a \le n-1 \Rightarrow 0 < n.k \le 2n-2$

$\Rightarrow k = 1$, $a^{-1} = n - a \in \mathbb{Z}_n$

$\overline{a^{-1}} \oplus \bar{a} = \overline{a^{-1} + a}$

$= \overline{a + a^{-1}}$

$= \bar{a} \oplus \overline{a^{-1}}$

$\Rightarrow$ The inverse element exists for all elements in $(\mathbb{Z}_n, \oplus)$.

Comment

$(\mathbb{Z}_n, \oplus)$ is a group.

Commutativity

$\bar{a} \oplus \bar{b} = \overline{a+b}$

$\bar{b} \oplus \bar{a} = \overline{b+a}$

$= \overline{a+b}$

$\Rightarrow \bar{a} \oplus \bar{b} \equiv \bar{b} \oplus \bar{a}$

$(\mathbb{Z}_n, \oplus)$ is commutative.

Comment

$(\mathbb{Z}_n, \oplus)$ is an Abelian group.

2.2) b)

Closure

$\bar{a} \otimes \bar{b}$

$\bar{b}$ \ $\bar{a}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{8}$
$\bar{3}$	$\bar{3}$	$\bar{6}$	$\bar{9}$	$\bar{12}$
$\bar{4}$	$\bar{4}$	$\bar{8}$	$\bar{12}$	$\bar{16}$

$\bar{6} = \{x \in \mathbb{Z} : x - 6 = 0 \pmod 5\}$

$= \{x \in \mathbb{Z} : (x-1) - 5 = 0 \pmod 5\}$

$= \{x \in \mathbb{Z} : x - 1 = 0 \pmod 5\}$

$= \bar{1} \in \mathbb{Z}_5 \setminus \{\bar{0}\}$

$\bar{8} = \{x \in \mathbb{Z} : x - 8 = 0 \pmod 5\}$

$= \{x \in \mathbb{Z} : (x-3) - 5 = 0 \pmod 5\}$

$= \{x \in \mathbb{Z} : x - 3 = 0 \pmod 5\}$

$= \bar{3} \in \mathbb{Z}_5 \setminus \{\bar{0}\}$

$\bar{9} = \{x \in \mathbb{Z} : x - 9 = 0 \pmod 5\}$

$= \{x \in \mathbb{Z} : (x-4) - 5 = 0 \pmod 5\}$

$= \{x \in \mathbb{Z} : x - 4 = 0 \pmod 5\}$

$= \bar{4} \in \mathbb{Z}_5 \setminus \{\bar{0}\}$

$\bar{12} = \{x \in \mathbb{Z} : x - 12 = 0 \pmod 5\}$

$= \{x \in \mathbb{Z} : (x-2) - (5)(2) = 0 \pmod 5\}$

$= \{x \in \mathbb{Z} : x - 2 = 0 \pmod 5\}$

$= \bar{2} \in \mathbb{Z}_5 \setminus \{\bar{0}\}$

$\overline{16} = \{x \in \mathbb{Z} : x - 16 = 0 \pmod 5\}$

$= \{x \in \mathbb{Z} : (x-1) - (5)(3) = 0 \pmod 5\}$

$= \{x \in \mathbb{Z} : |x-1| = 0 \pmod 5\}$

$= \bar{1} \in \mathbb{Z}_5 \setminus \{\bar{0}\}$

$\Rightarrow (\mathbb{Z}_5 \setminus \{\bar{0}\}, \otimes)$ is closed.

Neutral element

$\bar{a} \otimes \bar{e} = \bar{a}$

$\Rightarrow \overline{ae} = \bar{a}$

$\Rightarrow \bar{e} = \bar{1} \in \mathbb{Z}_5 \setminus \{\bar{0}\}$

$\bar{1} \otimes \bar{a} = \overline{|1|a|}$

$= \bar{a}$

$\Rightarrow (\mathbb{Z}_5 \setminus \{\bar{0}\}, \otimes)$ has neutral element $\bar{1}$.

Inverse element

Element	Inverse element
$\bar{1}$	$\bar{1}$
$\bar{2}$	$\bar{3}$
$\bar{3}$	$\bar{2}$
$\bar{4}$	$\bar{4}$

Associativity

$(\bar{a} \otimes \bar{b}) \otimes \bar{c} = \overline{ab} \otimes \bar{c}$

$= \overline{|ab|c}$

$= \overline{abc}$

$\bar{a} \otimes (\bar{b} \otimes \bar{c}) = \bar{a} \otimes \overline{bc}$

$= \overline{a|bc|}$

$= \overline{abc}$

$\Rightarrow (\bar{a} \otimes \bar{b}) \otimes \bar{c} \equiv \bar{a} \otimes (\bar{b} \otimes \bar{c})$

$(\mathbb{Z}_5 \setminus \{\bar{0}\}, \otimes)$ is associative.

Commutativity

$\bar{a} \otimes \bar{b} = \overline{ab}$

$\bar{b} \otimes \bar{a} = \overline{ba}$

$= \overline{ab}$

$\Rightarrow \bar{a} \otimes \bar{b} \equiv \bar{b} \otimes \bar{a}$

$(\mathbb{Z}_5 \setminus \{\bar{0}\}, \otimes)$ is commutative.

Conclusion

$(\mathbb{Z}_5 \setminus \{\bar{0}\}, \otimes)$ is an Abelian group.

2.2) c)

Counterexample

$\bar{2} \otimes \bar{4} = \bar{8}$

$= \{x \in \mathbb{Z} : x - 8 = 0 \pmod 8\}$

$= \{x \in \mathbb{Z} : x = 0 \pmod 8\} = \bar{0} \notin \mathbb{Z}_8 \setminus \{\bar{0}\}$

$(\mathbb{Z}_8, \otimes)$ is not closed $\therefore$ it is not a group.

2.2) d)

Let $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n \{\bar{0}\} : 1 \leq a, b, c \leq n-1$

Closure

Assume $(\mathbb{Z}_n \setminus \{\bar{0}\}, \otimes)$ is a group

$\Rightarrow (\mathbb{Z}_n \setminus \{\bar{0}\}, \otimes)$ is closed

$\Rightarrow \bar{a} \otimes \bar{b} \in \mathbb{Z}_n \setminus \{\bar{0}\}$

$\Rightarrow \overline{ab} \neq \bar{0}$

$\Rightarrow \{x \in \mathbb{Z} : x - ab = 0 \pmod n\} \neq \{x \in \mathbb{Z} : x = 0 \pmod n\}$

$\Rightarrow n \nmid ab$

$\Rightarrow n$ is prime

Proof: Consider $m \in \mathbb{N}$ such that m is prime.

$\Leftrightarrow \nexists a, b, k \in \mathbb{N}, \ a, b < m : ab = mk$

$\Leftrightarrow \forall a, b \in \mathbb{N}, \ a, b < m : m \nmid ab$

Assume n is prime.

$\Rightarrow \gcd(n, ab) = 1$

$\Rightarrow$ Bézout's theorem

$\exists p, q \in \mathbb{Z} : pn + qab = 1$

$\Rightarrow \exists p, q \in \mathbb{Z} : qab = pn + 1$

$\Rightarrow qab = 1 \pmod n$

If q is a multiple of n, then $ab = 1 \pmod n$.

If q is not a multiple of n, then

$n \nmid qab$

$\Rightarrow n \nmid ab$

$\Rightarrow ab \neq 0 \pmod n$

$\Rightarrow \bar{a} \otimes \bar{b} \neq \bar{0}$

Consider $\bar{a} \otimes \bar{b} = \overline{ab}$

ab can be written in the form $n \cdot q + r, \quad q, r \in \mathbb{Z}, \quad 0 \leq r < n$ $\therefore$ Euclidean division.

$\Rightarrow \bar{a} \otimes \bar{b} = \{x \in \mathbb{Z} : x - (n \cdot q + r) = 0 \pmod n\}$

$= \{x \in \mathbb{Z} : x - r = 0 \pmod n\}$

$= \bar{r} \in \mathbb{Z}_n$

$\Rightarrow (\mathbb{Z}_n \setminus \{\bar{0}\}, \otimes)$ closed if and only if $n \in \mathbb{N} \setminus \{0\}$ is prime.

Associativity

$$(\bar{a} \otimes \bar{b}) \otimes \bar{c} = \overline{ab} \otimes \bar{c}$$
$$= \overline{(ab)c}$$
$$= \overline{abc}$$

$$\bar{a} \otimes (\bar{b} \otimes \bar{c}) = \bar{a} \otimes \overline{bc}$$
$$= \overline{a(bc)}$$
$$= \overline{abc}$$

$\Rightarrow (\bar{a} \otimes \bar{b}) \otimes \bar{c} \equiv \bar{a} \otimes (\bar{b} \otimes \bar{c})$

$(\mathbb{Z}_n \setminus \{\bar{0}\}, \otimes)$ is associative.

Lemma: commutativity

$$\bar{a} \otimes \bar{b} = \overline{ab}$$

$$\bar{b} \otimes \bar{a} = \overline{ba}$$
$$= \overline{ab}$$

$\Rightarrow \bar{a} \otimes \bar{b} \equiv \bar{b} \otimes \bar{a}$

$(\mathbb{Z}_n \setminus \{\bar{0}\}, \otimes)$ is commutative.

Neutral element

$\bar{a} \otimes \bar{e} = \bar{e} \otimes \bar{a} = \bar{a}$

$\Rightarrow \overline{ae} = \bar{a}$

$\Rightarrow \bar{e} = \bar{1} \in \mathbb{Z}_n \setminus \{\bar{0}\}$

$\Rightarrow (\mathbb{Z}_n \setminus \{\bar{0}\}, \otimes)$ has neutral element $\bar{1}$.

Inverse element

Assume the inverse element exists $\forall \bar{a} \in \mathbb{Z}_n$

$\bar{a} \otimes \overline{a^{-1}} = \overline{a^{-1}} \otimes \bar{a} = \bar{1}$

$\Leftrightarrow \overline{aa^{-1}} = \bar{1}$

$\Leftrightarrow \{x \in \mathbb{Z} \mid x - aa^{-1} = 0 \pmod n\} = \{x \in \mathbb{Z} \mid x - 1 = 0 \pmod n\}$

$\Leftrightarrow aa^{-1} = 1 \pmod n$

$\Leftrightarrow \exists k, a^{-1} \in \mathbb{Z} : aa^{-1} + kn = 1$

$\Leftrightarrow \gcd(a, n) = 1$ (Bézout's theorem)

$\Leftrightarrow n$ is prime

The inverse element exists if and only if n is prime.

Conclusion

$(\mathbb{Z}_n \setminus \{\bar{0}\}, \otimes)$ is a group if and only if $n \in \mathbb{N} \setminus \{0\}$ is prime.