

1.2) a)

Closure

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

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

$a+b$ can be written in the form $nq+r$, $q, r \in \mathbb{Z}$, $0 \leq r < n$ \therefore Euclidean division

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

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

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

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

Associativity

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

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

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

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

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

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

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

(\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

$$\bar{a} \oplus \bar{a^{-1}} = \bar{0}$$

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

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

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

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

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

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

$0 < a < n-1 \Rightarrow 0 < nk \leq 2n-2$

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

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

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

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

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

Comment

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

Commutativity

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

$$\begin{aligned}\overline{b} \oplus \overline{a} &= \overline{b+a} \\ &= \overline{a+b}\end{aligned}$$

$$\Rightarrow \overline{a} \oplus \overline{b} = \overline{b} \oplus \overline{a}$$

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

Comment

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

2.2) b)

closure

$$\overline{a} \otimes \overline{b}$$

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

$$\begin{aligned}\overline{6} &= \{n \in \mathbb{Z} : n - 6 = 0 \pmod{5}\} \\ &= \{n \in \mathbb{Z} : (n-1) - 5 = 0 \pmod{5}\} \\ &= \{n \in \mathbb{Z} : n-1 = 0 \pmod{5}\} \\ &= \overline{1} \in \mathbb{Z}_5 \setminus \{\overline{0}\}\end{aligned}$$

$$\begin{aligned}\overline{8} &= \{n \in \mathbb{Z} : n - 8 = 0 \pmod{5}\} \\ &= \{n \in \mathbb{Z} : (n-3) - 5 = 0 \pmod{5}\} \\ &= \{n \in \mathbb{Z} : n-3 = 0 \pmod{5}\} \\ &= \overline{3} \in \mathbb{Z}_5 \setminus \{\overline{0}\}\end{aligned}$$

$$\begin{aligned}\overline{9} &= \{n \in \mathbb{Z} : n - 9 = 0 \pmod{5}\} \\ &= \{n \in \mathbb{Z} : (n-4) - 5 = 0 \pmod{5}\} \\ &= \{n \in \mathbb{Z} : n-4 = 0 \pmod{5}\} \\ &= \overline{4} \in \mathbb{Z}_5 \setminus \{\overline{0}\}\end{aligned}$$

$$\begin{aligned}\overline{12} &= \{n \in \mathbb{Z} : n - 12 = 0 \pmod{5}\} \\ &= \{n \in \mathbb{Z} : (n-2) - (5)(2) = 0 \pmod{5}\}\end{aligned}$$

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

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

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

$$= \{x \in \mathbb{Z} : (x - 1) - 15(3) \equiv 0 \pmod{5}\}$$

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

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

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

Neutral element

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

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

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

$$\bar{1} \otimes \bar{a} = \overline{(\bar{1})(\bar{a})}$$

$$= \bar{a}$$

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

$$\begin{aligned} (\bar{a} \otimes \bar{b}) \otimes \bar{c} &= \overline{\bar{a} \bar{b}} \otimes \bar{c} \\ &= \overline{(\bar{a} \bar{b}) \bar{c}} \\ &= \overline{\bar{a} \bar{b} \bar{c}} \end{aligned}$$

$$\begin{aligned} \bar{a} \otimes (\bar{b} \otimes \bar{c}) &= \bar{a} \otimes \overline{\bar{b} \bar{c}} \\ &= \overline{a (\bar{b} \bar{c})} \\ &= \overline{a \bar{b} \bar{c}} \end{aligned}$$

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

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

Commutativity

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

$$\begin{aligned} \bar{b} \otimes \bar{a} &= \overline{\bar{b} \bar{a}} \\ &= \overline{\bar{a} \bar{b}} \end{aligned}$$

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

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

Conclusion

$(\mathbb{Z}_8 \setminus \{\bar{0}\}, \otimes)$ is an Abelian group.

2.2) c)

Counterexample

$$\begin{aligned} \bar{2} \otimes \bar{4} &= \bar{8} \\ &= \{x \in \mathbb{Z} : x - 8 = 0 \pmod{8}\} \\ &= \{x \in \mathbb{Z} : x = 0 \pmod{8}\} = \bar{0} \notin \mathbb{Z}_8 \setminus \{\bar{0}\} \end{aligned}$$

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

2.2) d)

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

Closure

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

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

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

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

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

$\Rightarrow n \nmid ab$

$\Rightarrow n$ 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 Fermat'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 $\bar{a} \otimes \bar{b} = \bar{ab}$

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

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

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

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

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

Associativity

$$\begin{aligned} (\bar{a} \otimes \bar{b}) \otimes \bar{c} &= \bar{ab} \otimes \bar{c} \\ &= \overline{(ab)c} \\ &= \overline{abc} \end{aligned}$$

$$\begin{aligned} \bar{a} \otimes (\bar{b} \otimes \bar{c}) &= \bar{a} \otimes \overline{bc} \\ &= \overline{a(bc)} \\ &= \overline{abc} \end{aligned}$$

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

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

Lemma: commutativity

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

$$\begin{aligned} \bar{b} \otimes \bar{a} &= \bar{ba} \\ &= \bar{ab} \end{aligned}$$

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

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

Neutral element

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

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

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

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

Inverse element

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

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

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

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

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

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

$$\Leftrightarrow \gcd(a, n) = 1 \quad (\text{Bézout's theorem})$$

$\Leftrightarrow n$ is prime

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