2.2 Let n be in $\mathbb{N}\backslash\{0\}$. Let k, x be in $\mathbb{Z}$. We define the congruence class $\bar{k}$ of the integer k as the set

$$\bar{k} = x \in \mathbb{Z} | x - k = 0 \pmod{n}$$

$$= x \in \mathbb{Z} | \exists a \in \mathbb{Z} : (x - k = n.a)$$

We now define $\mathbb{Z}/n\mathbb{Z}$ (sometimes written as $\mathbb{Z}_n$) as the set of all congruence classes modulo n. Euclidean division implies that this set is a finite set containing n elements:

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, ..., \overline{n-1}\}$$

For all $\bar{a}, \bar{b} \in \mathbb{Z}_n$, we define

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

a. Show that $(\mathbb{Z}_n, \oplus)$ is a group. Is it Abelian?

Solution.

To prove that $(\mathbb{Z}_n, \oplus)$ is a group, we need to prove 4 conditions:

Closure, Associativity, Existence of neutral element, Existence of inverse element

Closure

We need to prove that $\forall \bar{a}, \bar{b} \in \mathbb{Z}_n : \bar{a} \oplus \bar{b} \in \mathbb{Z}_n$

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

$a+b < n \implies \overline{a+b} \in \mathbb{Z}_n$

$a+b > n \implies a+b$ can be expressed as the sum of a multiple of n,and a remainder r

$\implies a+b = m*n+r$ where $m, r \in \mathbb{Z}$ and $r < n$

$\implies \overline{a+b} = \overline{m*n+r}$

Since we are performing mod n,

$\overline{m*n+r} = \overline{r}$

$\implies \overline{a+b} = \overline{r}$

$r < n,$ so $\overline{a+b} \in \mathbb{Z}_n$

Closure proved.

Extra notes for clarity:

$\bar{0} = \{... - 2n, -n, 0, n, 2n, ...\}$

$\bar{1} = \{... - 2n+1, -n+1, 1, n+1, 2n+1, ...\}$

Associativity

To prove: $\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n : (\bar{a} \oplus \bar{b}) \oplus \bar{c} = \bar{a} \oplus (\bar{b} \oplus \bar{c})$

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

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

LHS = RHS. Associativity proved.

Existence of neutral element

To prove: $\exists \bar{e} \in \mathbb{Z}_n \forall \bar{a} \in \mathbb{Z}_n : \bar{a} \oplus \bar{e} = \bar{e} \oplus \bar{a} = \bar{a}$

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

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

This condition is satisfied if $e = n * m$ where $m \in \mathbb{Z}$

Neutral element exists.

Existence of inverse element

To prove: $\forall \bar{a} \in \mathbb{Z}_n \exists \bar{b} \in \mathbb{Z}_n : \bar{a} \oplus \bar{b} = \bar{b} \oplus \bar{a} = \bar{e}$

$\bar{a} \oplus \bar{b} = \bar{e} \implies \overline{a+b} = \overline{n * m}$ where $m \in \mathbb{Z}$

$\implies a = n - b$ for $m = 1$

Therefore, inverse exists.

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

To check if it is Abelian, we also need to check for commutativity.

To prove: $\forall \bar{a}, \bar{b} \in \mathbb{Z}_n : \bar{a} \oplus \bar{b} = \bar{b} \oplus \bar{a}$

$$
\begin{aligned}
\bar{a} \oplus \bar{b} &= \overline{a+b} \\
&= \overline{b+a} \qquad \text{since scalar addition is commutative} \\
&= \bar{b} \oplus \bar{a}
\end{aligned}
$$

Hence proved that $(\mathbb{Z}_n, \oplus)$ is an abelian group.

b. We now define another operation $\otimes$ for all $\overline{a}$ and $\overline{b}$ in $\mathbb{Z}_n$ as

$$\overline{a} \otimes \overline{b} = \overline{a \times b},$$

where $a \times b$ represents the usual multiplication in $\mathbb{Z}$.

Let n=5. Draw the times table of the elements of $\mathbb{Z}_5\backslash\{\overline{0}\}$ under $\otimes$, i.e., calculate the products $\overline{a} \otimes \overline{b}$ for all $\overline{a}$ and $\overline{b}$ in $\mathbb{Z}_5\backslash\{\overline{0}\}$ under $\otimes$. Conclude that $(\mathbb{Z}_5\backslash\{\overline{0}\}, \otimes)$ is an abelian group.

Solution.

$\mathbb{Z}_5\backslash\{\overline{0}\} = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$

$\otimes$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

To prove that $(\mathbb{Z}_5\backslash\{\overline{0}\}, \otimes)$ is an abelian group, we need to prove 5 conditions:

Closure, Associativity, Existence of neutral element, Existence of inverse element, and Commutativity.

Closure

We can see in the table that for all $\overline{a}, \overline{b} \in \mathbb{Z}_5\backslash\{\overline{0}\}, \overline{a} \otimes \overline{b} \in \mathbb{Z}_5\backslash\{\overline{0}\}$

Associativity

Let $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_5 \backslash \{\overline{0}\}$

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

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

$$= \overline{a \times (b \times c)} \qquad \text{because scalar multiplication is associative}$$

$$= \overline{a} \otimes \overline{b \times c}$$

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

Associativity proved.

Existence of neutral element

We can see in the table, from the first row and the first column, that

$\overline{x} \otimes \overline{1} = \overline{1} \otimes \overline{x} = \overline{x}$

Therefore $\overline{1}$ is the neutral element.

Existence of inverse element

We can see in the table that every row and every column in the table contains at least one $\overline{1}$, such that the result of the operation between the elements specific by the i^{th} row and the j^{th} column is $\overline{1}$.

Also, the result of the operation between the elements specific by the j^{th} row and the i^{th} column is also $\overline{1}$. The table is symmetric.

Commutativity

The table is symmetric. So the operation is commutative over $\mathbb{Z}_5 \backslash \{0\}$.

Hence proved that $(\mathbb{Z}_5\backslash\{\overline{0}\}, \otimes)$ is an abelian group.‘

c. Show that $(\mathbb{Z}_8\backslash\{\overline{0}\}, \otimes)$ is not a group.

Solution.

Times table for $\mathbb{Z}_8\backslash\{\overline{0}\}$ under $\otimes$:

$\otimes$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$
$\overline{3}$	$\overline{3}$	$\overline{6}$	$\overline{1}$	$\overline{4}$	$\overline{7}$	$\overline{2}$	$\overline{5}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$
$\overline{5}$	$\overline{5}$	$\overline{2}$	$\overline{7}$	$\overline{4}$	$\overline{1}$	$\overline{6}$	$\overline{3}$
$\overline{6}$	$\overline{6}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{7}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Since $\overline{0} \notin \mathbb{Z}_8\backslash\{\overline{0}\}$, Closure property is violated, and $(\mathbb{Z}_8\backslash\{\overline{0}\}, \otimes)$ is not a group.

d. We recall that the Bézout theorem states that two integers a and b are relatively prime (i.e., $gcd(a, b) = 1$, if and only if there exist two integers u and v such that $au + bv = 1$. Show that $(\mathbb{Z}_n\backslash\{\overline{0}\}, \otimes)$ is a group if and only if $n \in \mathbb{N}\backslash\{0\}$ is prime.

Solution.

To prove: $(\mathbb{Z}_n\backslash\{\overline{0}\}, \otimes)$ is a group $\iff$ $n \in \mathbb{N}\backslash\{0\}$ is prime

So, we need to prove two statements:

$(\mathbb{Z}_n\backslash\{\overline{0}\}, \otimes)$ is a group $\Longrightarrow n \in \mathbb{N}\backslash\{0\}$ is prime

and

$n \in \mathbb{N}\backslash\{0\}$ is prime $\Longrightarrow (\mathbb{Z}_n\backslash\{\overline{0}\}, \otimes)$ is a group

To prove that $(\mathbb{Z}_n\backslash\{\overline{0}\}, \otimes)$ is a group, we need to prove 4 conditions:

Closure, Associativity, Existence of neutral element and Existence of inverse element

Closure

If n is not prime, then it can be factorized into a and b such that $a \times b = n$. Since $a, b < n$, $(a \times b) \mod n = 0$ and closure property is violated because $\overline{0} \notin \mathbb{Z}_n\backslash\{\overline{0}\}$.

So, we proved that $\neg$ n is prime $\Longrightarrow \neg$ closure property holds

$\Longrightarrow$ (closure property holds $\Longrightarrow$ n is prime)

Also, if n is prime, then $n > (a \times b) \mod n > 0$, and closure property holds.

$\Longrightarrow$ (n is prime $\Longrightarrow$ closure property holds)

So we can say (n is prime $\iff$ closure property holds)

Associativity

Let $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n \backslash \{\overline{0}\}$

$$
\begin{aligned}
&\overline{a} \otimes (\overline{b} \otimes \overline{c}) \\
&= \overline{a} \otimes \overline{(b \times c)} \\
&= \overline{a \times (b \times c)} \\
&= \overline{(a \times b) \times c} && \text{Scalar multiplication is associative} \\
&= \overline{(a \times b)} \otimes \overline{c} \\
&= (\overline{a} \otimes \overline{b}) \otimes \overline{c}
\end{aligned}
$$

Associativity proved.

Existence of identity element

Let $\overline{a} \in \mathbb{Z}_n \backslash \{\overline{0}\}$, and let $\overline{e}$ be the identity element.

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

$\implies \overline{a \times e} = \overline{a} = \overline{e \times a}$

If $e = 1$, above condition is satisfied.

Identity element is 1.

Existence of inverse element

To prove: $\forall \overline{a} \in \mathbb{Z}_n \backslash \{\overline{0}\}, \exists \overline{b} \in \mathbb{Z}_n \backslash \{\overline{0}\} : \overline{a} \otimes \overline{b} = \overline{1}$

If n is prime, then n and a are coprime.

As per Bézout theorem, this implies that

$$au + nv = 1$$

$$\implies au = 1 - nv$$

$$\implies \overline{au} = \overline{1 - nv} = \overline{1}$$

Case 1: $n > u \geq 1$ No problem in this case.

Case 2: $u \geq n$, u can be represented as $m \times n + r$ where $m \in \mathbb{W}, n > r \geq 0$

In this case, $\overline{au} = \overline{a(mn + r)} = \overline{amn + ar} = \overline{ar}$

$r \neq 0$ because that would make $\overline{au} = \overline{0}$

Therefore, r is the inverse here, where $n > r > 0$.

Case 3: $u < 0$

u can be represented as $r - m \times n$ where $m \in \mathbb{W}, n > r > 0$

eg. $u = -11$, $n = 5$, $-11 = 4 - 5 \times 3$

Therefore, $\overline{au} = \overline{a(r - mn)} = \overline{ar - amn} = \overline{ar}$

Therefore, r is the inverse here.

Therefore, if n is prime, every element has an inverse.

If n is not prime, then n can be factorized into a and b such that $n = a \times b$, $n > a, b > 1$

Now, let x be the inverse of a.

$$\implies \overline{a} \otimes \overline{x} = \overline{1}$$
$$\implies \overline{a} \otimes \overline{x} \otimes \overline{b} = \overline{1} \otimes \overline{b}$$
$$\implies \overline{a \times x \times b} = \overline{b}$$
$$\implies \overline{n \times x} = \overline{1}$$
$$\implies \overline{0} = \overline{1}$$

This is a contradiction, therefore, for any factors of n, inverse does not exist.

Therefore, if n is not prime, every element does not have an inverse, implying that if inverse exists for every element, n is prime.

We have proved the following : n is prime $\iff$ inverse exists for every element.

Commutativity

$\forall \overline{a}, \overline{b} \in \mathbb{Z}_n \backslash \{\overline{0}\}$

$$\overline{a} \otimes \overline{b} = \overline{a \times b}$$
$$= \overline{b \times a} \qquad \text{scalar multiplication is commutative}$$
$$= \overline{b} \otimes \overline{a}$$

Commutativity proved.

So, for the properties of closure and existence of inverse, we have proved that n is prime $\iff$ closure and existence of inverse.

Other properties are not impacted by n being prime. So, we have proved that $(\mathbb{Z}_n\backslash\{\overline{0}\}, \otimes)$ is a group if and only if $n \in \mathbb{N}\backslash\{0\}$ is prime.