Exercise: Questions **1, 3, 4** are assessed.
Suggestion for the MMT: Questions 2(a), 2(b), 2(c)

1. We consider $(\mathbb{R}\backslash\{-1\},\star)$ where where

$$a\star b := ab + a + b, \qquad a, b \in \mathbb{R}\backslash\{-1\} \tag{1}$$

(a) Show that $(\mathbb{R}\backslash\{-1\},\star)$ is an Abelian group
Exam standard. **[5 Marks]**

(b) Solve

$$3\star x \star x = 15$$

in the Abelian group $(\mathbb{R}\backslash\{-1\},\star)$, where $\star$ is defined in (1).
[2 Marks]

(a) i. First, we show that $\mathbb{R}\backslash\{-1\}$ is closed under $\star$: For all $a, b \in \mathbb{R}\backslash\{-1\}$:

$$a\star b = ab + a + b + 1 - 1 = \underbrace{(a+1)}_{\neq 0}\underbrace{(b+1)}_{\neq 0} - 1 \neq -1$$
$$\Rightarrow a\star b \in \mathbb{R}\backslash\{-1\}$$

ii. Next, we show the group axioms

- **Associativity:** For all $a, b, c \in \mathbb{R}\backslash\{-1\}$:

$$\begin{aligned}(a\star b)\star c &= (ab + a + b)\star c \\ &= (ab + a + b)c + (ab + a + b) + c \\ &= abc + ac + bc + ab + a + b + c \\ &= a(bc + b + c) + a + (bc + b + c) \\ &= a\star(bc + b + c) \\ &= a\star(b\star c)\end{aligned}$$

- **Commutativity:**

$$\forall a, b \in \mathbb{R}\backslash\{-1\} : a\star b = ab + a + b = ba + b + a = b\star a$$

- **Neutral Element:** $n = 0$ is the neutral element since

$$\forall a \in \mathbb{R}\backslash\{-1\} : a\star 0 = a = 0\star a$$

- **Inverse Element:** We need to find $\bar{a}$, such that $a\star\bar{a} = 0 = \bar{a}\star a$.

$$\begin{aligned}\bar{a}\star a = 0 &\Leftrightarrow \bar{a}a + a + \bar{a} = 0 \\ &\Leftrightarrow \bar{a}(a+1) = -a \\ &\overset{a\neq -1}{\Leftrightarrow} \bar{a} = -\frac{a}{a+1} = -1 + \frac{1}{a+1} \neq -1 \in \mathbb{R}\backslash\{-1\}\end{aligned}$$

(b)

$$\begin{aligned} 3 \star x \star x = 15 &\Leftrightarrow 3 \star (x^2 + x + x) = 15 \\ &\Leftrightarrow 3x^2 + 6x + 3 + x^2 + 2x = 15 \\ &\Leftrightarrow 4x^2 + 8x - 12 = 0 \\ &\Leftrightarrow (x-1)(x+3) = 0 \\ &\Leftrightarrow x \in \{-3, 1\} \end{aligned}$$

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

$$\begin{aligned} \overline{k} &= \{x \in \mathbb{Z} \mid x - k = 0 \pmod{n}\} \\ &= \{x \in \mathbb{Z} \mid (\exists a \in \mathbb{Z})\colon (x - k = n \cdot a)\}. \end{aligned}$$

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

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

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

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

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

- Let $\overline{a}, \overline{b}$ be in $\mathbb{Z}_n$. We have:

$$\begin{aligned} \overline{a} \oplus \overline{b} &= \overline{a+b} \\ &= \overline{(a+b) \mod n} \end{aligned}$$

by definition of the congruence class, and since $[(a+b) \bmod n] \in \{0, \ldots, n-1\}$, it follows that $\overline{a} \oplus \overline{b} \in \mathbb{Z}_n$. Thus, $\mathbb{Z}_n$ is closed under $\oplus$.

- Let $\overline{c}$ be in $\mathbb{Z}_n$. We have:

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

so $\oplus$ is associative.

- We have

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

so $\overline{0}$ is the neutral element for $\oplus$.

- We have

$$\overline{a} + \overline{(-a)} = \overline{a-a} = \overline{0} = \overline{(-a)} + \overline{a}$$

and we know that $\overline{(-a)}$ is equal to $\overline{(-a) \bmod n}$ which belongs to $\mathbb{Z}_n$ and is thus the inverse of $\overline{a}$.

- Finally, the commutativity of $(\mathbb{Z}_n, \oplus)$ follows from that of $(\mathbb{Z}, +)$ since we have:

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

which shows 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 $\mathbb{Z}_5 \setminus \{\overline{0}\}$ under $\otimes$, i.e., calculate the products $\overline{a} \otimes \overline{b}$ for all $\overline{a}$ and $\overline{b}$ in $\mathbb{Z}_5 \setminus \{\overline{0}\}$.
Hence, show that $\mathbb{Z}_5 \setminus \{\overline{0}\}$ is closed under $\otimes$ and possesses a neutral element for $\otimes$. Display the inverse of all elements in $\mathbb{Z}_5 \setminus \{\overline{0}\}$ under $\otimes$. Conclude that $(\mathbb{Z}_5 \setminus \{\overline{0}\}, \otimes)$ is an Abelian group.
Let us calculate the times table of $\mathbb{Z}_5 \setminus \{\overline{0}\}$ under $\otimes$:

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

We can notice that all the products are in $\mathbb{Z}_5 \setminus \{\overline{0}\}$, and that in particular, none of them is equal to $\overline{0}$. Thus, $\mathbb{Z}_5 \setminus \{\overline{0}\}$ is closed under $\otimes$. The neutral element is $\overline{1}$ and we have $(\overline{1})^{-1} = \overline{1}$, $(\overline{2})^{-1} = \overline{3}$, $(\overline{3})^{-1} = \overline{2}$, and $(\overline{4})^{-1} = \overline{4}$.
Associativity and commutativity are straightforward and $(\mathbb{Z}_5 \setminus \{\overline{0}\}, \otimes)$ is an Abelian group.

(c) Show that $(\mathbb{Z}_8 \setminus \{\overline{0}\}, \otimes)$ is not a group.
The elements $\overline{2}$ and $\overline{4}$ belong to $\mathbb{Z}_8 \setminus \{\overline{0}\}$, but their product $\overline{2} \otimes \overline{4} = \overline{8} = \overline{0}$ does not. Thus, this set is not closed under $\otimes$ and is not a group.

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

- Let us assume that n is not prime and can thus be written as a product $n = a \times b$ of two integers a and b in $\{2, \ldots, n-1\}$. Both elements $\overline{a}$ and $\overline{b}$ belong to $\mathbb{Z}_n \setminus \{\overline{0}\}$ but their product $\overline{a} \otimes \overline{b} = \overline{n} = \overline{0}$ does not. Thus, this set is not closed under $\otimes$ and $(\mathbb{Z}_n \setminus \{\overline{0}\}, \otimes)$ is not a group.
- Let n be a prime number. Let $\overline{a}$ and $\overline{b}$ be in $\mathbb{Z}_n \setminus \{\overline{0}\}$ with a and b in $\{1, \ldots, n-1\}$. As n is prime, we know that a is relatively prime to n, and so is b. Let us then take four integers u, v, u' and v' such that

$$au + nv = 1$$

$$bu' + nv' = 1$$

We thus have: $(au + nv)(bu' + nv') = 1$ which we can rewrite as:

$$ab(uu') + n(auv' + vbu' + nvv') = 1$$

By virtue of Bézout theorem, this implies that ab and n are relatively prime, which ensures that the product $\overline{a} \otimes \overline{b}$ is not equal to $\overline{0}$ and belongs to $\mathbb{Z}_n \setminus \{\overline{0}\}$, which is thus closed under $\otimes$.
The associativity and commutativity of $\otimes$ are straightforward, but we need to show that every element has an inverse. First, the neutral element is $\overline{1}$. Let us again consider an element $\overline{a}$ in $\mathbb{Z}_n \setminus \{\overline{0}\}$ with a in $\{1, \ldots, n-1\}$. As a and n are coprime, Bézout theorem enables us to define two integers u and v such that

$$au + nv = 1$$

which implies: $au = 1 - nv$ and thus:

$$au = 1 \mod n$$

which means that $\overline{a} \otimes \overline{u} = \overline{au} = \overline{1}$, or that $\overline{u}$ is the inverse of $\overline{a}$. Overall, $(\mathbb{Z}_n \setminus \{\overline{0}\}, \otimes)$ is an Abelian group. Note that Bézout theorem ensures the existence of an inverse without yielding its explicit value, which is the purpose of the extended Euclidean algorithm.

3. Consider the set G of 3×3 matrices defined as:

$$G = \left\{ \begin{bmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix} \in \mathbb{R}^{3\times 3} \,\middle|\, x, y, z \in \mathbb{R} \right\}$$

We define $\cdot$ as the standard matrix multiplication.
Determine whether

- G is closed under $\cdot$
- $(G, \cdot)$ is associative
- $(G, \cdot)$ is commutative
- $(G, \cdot)$ possesses a neutral element

Justify your answers. **[8 Marks]**

- **Closure:** Let a, b, c, x, y and z be in $\mathbb{R}$ and let us define $\boldsymbol{A}$ and $\boldsymbol{B}$ in G as:

$$\boldsymbol{A} = \begin{bmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix}, \qquad \boldsymbol{B} = \begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix}$$

We have:

$$A \cdot B = \begin{bmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+x & c+xb+z \\ 0 & 1 & b+y \\ 0 & 0 & 1 \end{bmatrix}$$

But $a+x$, $b+y$ and $c+xb+z$ are in $\mathbb{R}$, so we have $\boldsymbol{A} \cdot \boldsymbol{B} \in G$ and thus G is closed under matrix multiplication.

- **Associativity** Let α, β and γ be in $\mathbb{R}$ and let $\boldsymbol{C}$ in G be defined as:

$$\boldsymbol{C} = \begin{bmatrix} 1 & \alpha & \gamma \\ 0 & 1 & \beta \\ 0 & 0 & 1 \end{bmatrix}$$

We have:

$$(\boldsymbol{A} \cdot \boldsymbol{B}) \cdot \boldsymbol{C} = \begin{bmatrix} 1 & a+x & c+xb+z \\ 0 & 1 & b+y \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & \alpha & \gamma \\ 0 & 1 & \beta \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & \alpha+a+x & \gamma+\alpha\beta+x\beta+c+xb+z \\ 0 & 1 & \beta+b+y \\ 0 & 0 & 1 \end{bmatrix}$$

And similarly:

$$\begin{aligned} \boldsymbol{A} \cdot (\boldsymbol{B} \cdot \boldsymbol{C}) &= \begin{bmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & \alpha+a & \gamma+\alpha\beta+c \\ 0 & 1 & \beta+b \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & \alpha+a+x & \gamma+\alpha\beta+x\beta+c+xb+z \\ 0 & 1 & \beta+b+y \\ 0 & 0 & 1 \end{bmatrix} \\ &= (\boldsymbol{A} \cdot \boldsymbol{B}) \cdot \boldsymbol{C} \end{aligned}$$

Thus $\cdot$ is associative.

- **Neutral Element:** For all $\boldsymbol{A}$ in G, we have: $\boldsymbol{I}_3 \cdot \boldsymbol{A} = \boldsymbol{A} = \boldsymbol{A} \cdot \boldsymbol{I}_3$ and thus $\boldsymbol{I}_3$ is the neutral element.
- **Commutativity:** Let us prove that $\cdot$ is not commutative. Let us consider the following matrices $\boldsymbol{X}$ and $\boldsymbol{Y}$ in G defined as follows:

$$\boldsymbol{X} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \qquad \boldsymbol{Y} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

We have:

$$\boldsymbol{X} \cdot \boldsymbol{Y} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\boldsymbol{Y} \cdot \boldsymbol{X} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \neq \boldsymbol{X} \cdot \boldsymbol{Y}$$

And thus $\cdot$ is not commutative.

4. Compute the following matrix products:
   [5 Marks]

(a)

$$\begin{bmatrix}1 & 2\\4 & 5\\7 & 8\end{bmatrix}\begin{bmatrix}1 & 1 & 0\\0 & 1 & 1\\1 & 0 & 1\end{bmatrix}$$

This matrix product is not defined. Highlight that the neighboring dimensions have to fit (i.e., $m \times n$ matrices need to be multiplied by $n \times p$ (from the right) or $k \times m$ matrices (from the left).)

(b)

$$\begin{bmatrix}1 & 2 & 3\\4 & 5 & 6\\7 & 8 & 9\end{bmatrix}\begin{bmatrix}1 & 1 & 0\\0 & 1 & 1\\1 & 0 & 1\end{bmatrix} = \begin{bmatrix}4 & 3 & 5\\10 & 9 & 11\\16 & 15 & 17\end{bmatrix}$$

(c)

$$\begin{bmatrix}1 & 1 & 0\\0 & 1 & 1\\1 & 0 & 1\end{bmatrix}\begin{bmatrix}1 & 2 & 3\\4 & 5 & 6\\7 & 8 & 9\end{bmatrix} = \begin{bmatrix}5 & 7 & 9\\11 & 13 & 15\\8 & 10 & 12\end{bmatrix}$$

(d)

$$\begin{bmatrix}1 & 2 & 1 & 2\\4 & 1 & -1 & -4\end{bmatrix}\begin{bmatrix}0 & 3\\1 & -1\\2 & 1\\5 & 2\end{bmatrix} = \begin{bmatrix}14 & 6\\-21 & 2\end{bmatrix}$$

(e)

$$\begin{bmatrix}0 & 3\\1 & -1\\2 & 1\\5 & 2\end{bmatrix}\begin{bmatrix}1 & 2 & 1 & 2\\4 & 1 & -1 & -4\end{bmatrix} = \begin{bmatrix}12 & 3 & -3 & -12\\-3 & 1 & 2 & 6\\6 & 5 & 1 & 0\\13 & 12 & 3 & 2\end{bmatrix}$$