2. Which of the following multiplication tables defines a group on the set $G = \{a, b, c, d\}$?

(a)

$\circ$	a	b	c	d
a	a	c	d	a
b	b	b	c	d
c	c	d	a	b
d	d	a	b	c

This **is not** a group. The table shows that the equation $b \circ x = a$ has no solution. If this were a group, we would have a solution as follows:

$$\begin{aligned} b \circ x &= a \\ b^{-1} \circ (b \circ x) &= b^{-1} \circ a \\ (b^{-1} \circ b) \circ x &= b^{-1} \circ a \\ e \circ x &= b^{-1} \circ a \\ x &= b^{-1} \circ a. \end{aligned}$$

(b)

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

This **is** a group! Just let $a = (0, 0)$, $b = (0, 1)$, $c = (1, 0)$ and $d = (1, 1)$, and this is the table for $\mathbb{Z}_2 \times \mathbb{Z}_2$. (See Table 3.5 in the text.)

(c)

$\circ$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

This **is** a group! Just let $a = 0$, $b = 1$, $c = 2$ and $d = 3$, and this is the table for $\mathbb{Z}_4$.

(d)

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c	c	b	a	d
d	d	d	b	c

This **is not** a group. If it were, the identity would have to be a, as we have $a \circ x = x$ for each $x \in G$. But then d has no inverse, for the table shows $d \circ x \neq a$ for each $x \in G$.

7. Let $S = \mathbb{R} \setminus \{-1\}$ and define a binary operation on S as $a * b = a + b + ab$. Prove that $(S, *)$ is an abelian group.

We should first check that $*$ is really a valid binary operation on the set $S = \mathbb{R} \setminus \{-1\}$. Suppose $a, b \in S = \mathbb{R} \setminus \{-1\}$. Then a and b are real numbers, so certainly $a * b = a + b + ab$ is a real number too. We just need to show that it is not equal to -1, that is, $a * b \in \mathbb{R} \setminus \{-1\}$. Suppose to the contrary that $a * b = a + b + ab = -1$. Now we have

$$\begin{aligned} a + b + ab &= -1 \\ a + b(1 + a) &= -1 \\ b(1 + a) &= -1 - a \\ b &= \frac{-1 - a}{1 + a} \qquad \text{(division OK, since } a \neq -1) \\ b &= -1. \end{aligned}$$

But $b = -1$ contradicts the fact that $b \in \mathbb{R} \setminus \{-1\}$. Therefore we conclude $a * b \neq -1$, so $a * b \in S = \mathbb{R} \setminus \{-1\}$. This shows that $*$ is indeed a binary operation on S.

Next we are going to show that $(S, *)$ satisfies the group axioms.

1. Note that $*$ is associative, as follows.

$$\begin{aligned} (a * b) * c &= (a + b + ab) * c \\ &= (a + b + ab) + c + (a + b + ab)c \\ &= a + b + ab + cac + bc + abc \\ &= a + (b + c + bd) + a(b + c + bc) \\ &= a * (b + c + bc) \\ &= a * (b * c) \end{aligned}$$

2. Notice that 0 is an identity because $a * 0 = a + 0 + a \cdot 0 = a$ and $0 * a = 0 + a + 0 \cdot a = a$ for each $a \in S$.
3. Notice that each element $a \in S$ has an inverse $a^{-1} = \frac{-a}{1+a}$ because

$$\begin{aligned} a * \frac{-a}{1+a} &= a + \frac{-a}{1+a} + a\frac{-a}{1+a} \\ &= \frac{a(1+a)}{1+a} + \frac{-a}{1+a} + \frac{-a^2}{1+a} \\ &= 0. \end{aligned}$$

(Recall that 0 is the identity.) Likewise we have $\frac{-a}{1+a} * a = 0$.

We've shown that $(S, *)$ is associative, has an identity element, and each element has an inverse. Thus it is a group.

Note that $a * b = a + b + ab = b + a + ba = b * a$. Since $a * b = b * a$, the group is abelian..

10. Prove that the set of matrices of the form $\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$ is a group under matrix multiplication.

Note that the product of two matrices of the given form has the same form (i.e. 1's on the diagonal and 0's below the diagonal):

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x' & y' \\ 0 & 1 & z' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x + x' & y + y' + xz' \\ 0 & 1 & z + z' \\ 0 & 0 & 1 \end{pmatrix}$$

It follows that matrix multiplication is a well-defined binary operation on the set of all matrices of the given form.

Let's check that this is a group

1. We know from linear algebra that matrix multiplication is associative, so the given binary operation is automatically associative.
2. If we let $x = y = z = 0$ then it is clear that the identity matrix I has the above form. Thus I is an identity element, as $IA = AI$ for each matrix A.
3. Finally, note that each matrix of the above form is invertible, as its determinant is 1, so it is invertible. Moreover, we have

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -x & xz - y \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{pmatrix},$$

which is also of the given form.

Thus the set of all such matrices is a group, for matrix multiplication on it is associative, there is an identity, and there is an inverse of each matrix.

13. Show that $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ is a group under the operation of multiplication.

Given $a, b, c \in \mathbb{R}^*$, we have $a(bc) = (ab)c$ because multiplication of real numbers is associative. Also, we have $1 \in \mathbb{R}^*$, and $1a = a1 = a$, so $\mathbb{R}^*$ has an identity $e = 1$. Finally, given any $a \in \mathbb{R}^* = \mathbb{R} \setminus \{0\}$, it follows that $a \neq 0$, so the element $a^{-1} = \frac{1}{a}$ is defined. As $aa^{-1} = a\frac{1}{a} = 1$ and $a^{-1}a = 1$, it follows that each element $a \in \mathbb{R}^*$ has an inverse a^{-1}.

Thus $\mathbb{R}^*$ is a group.

14. Given the groups $\mathbb{R}^*$ and $\mathbb{Z}$, let $G = \mathbb{R}^* \times \mathbb{Z}$. Define a binary operation on this set as $(a, m) \circ (b, n) = (ab, m + n)$. Show that G is a group under this operation.

Let's verify each of the three group axioms.

1. Note that $\circ$ is associative, as follows.

$$\begin{aligned} [(a, m) \circ (b, n)] \circ (c, k) &= (ab, m + n) \circ (c, k) \\ &= (abc, m + n + k) \\ &= (a, m) \circ (bc, n + k) \\ &= (a, m) \circ [(b, n) \circ (c, k)] \end{aligned}$$

2. Notice that (1,0) is an identity because $(a, m) \circ (1, 0) = (a \cdot 1, m + 0) = (a, m)$ and $(1, 0) \circ (a, m) = (1 \cdot a, 0 + m) = (a, m)$ for each $(a, m) \in G$.
3. Notice that each element $(a, m) \in G$ has an inverse $(\frac{1}{a}, -m)$ because $(a, m) \circ (\frac{1}{a}, -m) = (1, 0)$ and $(\frac{1}{a}, -m) \circ (a, m) = (1, 0)$. (Recall that $(1, 0)$ is the identity.)

We've shown that $(G, \circ)$ is associative, has an identity element $(1, 0)$, and each element has an inverse. Thus it is a group.

21. For each $a \in \mathbb{Z}_n$, find a b for which $a + b \equiv b + a \equiv 0 \pmod{n}$.

Just let $b = [n - a]$. Then $[a] + [b] = [a] + [n - a] = [a + n - a] = [n] = [0]$.
This means $a + b \equiv 0 \pmod{n}$.