1) Find the orders of each element of the additive group $\mathbb{Z}/12\mathbb{Z}$.

$\rightarrow$ For any group $(G, *)$ the order of $a \in G$ is defined as the least positive integer n such that $a^n = \mathbb{1}$. For the additive group $\mathbb{Z}/12\mathbb{Z}$, we must find n such that $\overline{na} = \bar{0}$. The following table summarizes the orders of each integer.

element	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$	$\overline{10}$	$\overline{11}$
order	1	12	6	4	3	12	2	12	3	4	6	12

2) Find the orders of the following elements of the multiplicative group $(\mathbb{Z}/36\mathbb{Z})^\times$: $\bar{1}$, $\overline{-1}$, $\bar{5}$, $\overline{-13}$, $\overline{17}$.

$\rightarrow$ To find the orders of the elements of the group $(\mathbb{Z}/36\mathbb{Z})^\times$, we determine the least n such that $\bar{a}^n = \overline{a^n} = \bar{1}$. They are as follows:

$$\begin{aligned} \text{order}\left(\bar{1}\right) &= 1 \\ \text{order}\left(\overline{-1}\right) &= 2 \\ \text{order}\left(\bar{5}\right) &= 6 \\ \text{order}\left(\overline{-13}\right) &= 6 \\ \text{order}\left(\overline{17}\right) &= 2 \end{aligned}$$

3) Let $(A, \star)$ and $(B, \diamond)$ be groups. Let $A \times B$ be the Cartesian product of A and B. Define an operation $*$ on $A \times B$ by

$$(a_1, b_1) * (a_2, b_2) = (a_1 \star a_2, b_1 \diamond b_2).$$

Show that $(A \times B, *)$ is a group.

<u>Proof</u>
We prove the following properties:

i) Observe that

$$\begin{aligned} [(a_1, b_1) * (a_2, b_2)] * (a_3, b_3) &= ((a_1 \star a_2) \star a_3, (b_1 \diamond b_2) \diamond b_3) \\ &= (a_1 \star (a_2 \star a_3), b_1 \diamond (b_2 \diamond b_3)) \\ &= (a_1, b_1) * [(a_2, b_2) * (a_3, b_3)] \end{aligned}$$

since $\star$ and $\diamond$ are associative binary operations on A and B, respectively.

ii) Since $(A, \star)$ and $(B, \diamond)$ are groups, they must have identities $\mathbb{1}_{(A,\star)}$ and $\mathbb{1}_{(B,\diamond)}$. Thus, we see that $(A \times B, *)$ has an identity element $\mathbb{1} = (\mathbb{1}_{(A,\star)}, \mathbb{1}_{(B,\diamond)})$ since $(a, b) * \mathbb{1} = (a \star \mathbb{1}_{(A,\star)}, b \diamond \mathbb{1}_{(B,\diamond)}) = (a, b)$.

iii) Finally, since each element $a \in A$ and $b \in B$ have unique inverses a^{-1} and b^{-1} under $\star$ and $\diamond$, respectively, we see that $(a, b) \in A \times B$ has inverse (a^{-1}, b^{-1}) under $*$, observing that $(a, b) * (a^{-1}, b^{-1}) = (a \star a^{-1}, b \diamond b^{-1}) = (\mathbb{1}_{(A,\star)}, \mathbb{1}_{(B,\diamond)}) = \mathbb{1}$.

$\blacksquare$

4) Let A be the set of 2×2 matrices with real number entries. Let

$$M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and let

$$B = \{X \in A : XM = MX\}$$

1) Determine which of the following elements of A lies in B

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$\rightarrow$ Observe the following:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} M = M^2 = M \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} M = M \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} M = \mathbb{1}_{2\times 2} M = M \mathbb{1}_{2\times 2} = M \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

Hence, the matrices

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

are elements of B.

2) Prove that if $P, Q \in B$, then $P + Q \in B$.

Proof

Notice that $PM = MP$ and $QM = MQ$. Hence, $PM + QM = MP + MQ$ or $(P+Q)M = M(P+Q)$.

■

3) Prove that if $P, Q \in B$, then $PQ \in B$.

Proof
Notice that $PM = MP$. Multiplying on the right by Q, we have $PMQ = MPQ$. Since $QM = MQ$, we have $PQM = MPQ$.

■

4) Is the set B with matrix addition a group?

Proof
We show that B is a group under matrix addition. Since B is a set of matrices and matrix addition is associative, it immediately follows that B is associative under matrix addition. Additionally, we have trivially that

$$\mathbb{1}_+ = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Finally, it is easy to see that for any matrix P that its inverse is $-P$ since $P + (-P) = P - P = 0$ (the zero matrix).

■

5) Is the set B with matrix multiplication a group?

Proof
It is easy to observe that B is not a group under matrix multiplication. Matrix multiplication is associative generally and

$$\mathbb{1}_\times = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

is the identity for 2×2 matrix multiplication, but we cannot find a unique inverse for each $P \in B$ since P is invertible iff $\det(P) \neq 0$. A counterexample may be

$$P = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

which has a determinant which is trivally zero.

■

Note: If we impose an additional restriction on B such that only matrices which are invertible are elements of B, then B would be a group under matrix multiplication.

5[2.1.2]) Let θ be a real number and define

$$R_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}.$$

(a) R_θ is called a rotation matrix. Can you explain why?

Consider rotating a point $(x, y) = (r\cos\phi, r\sin\phi)$ to a point (x', y') by an angle θ. Then

$$\begin{aligned}\begin{bmatrix} x' \\ y' \end{bmatrix} &= \begin{bmatrix} r\cos(\phi+\theta) \\ r\sin(\phi+\theta) \end{bmatrix} = \begin{bmatrix} r\cos\phi\cos\theta - r\sin\phi\sin\theta \\ r\cos\phi\sin\theta + r\sin\phi\cos\theta \end{bmatrix} = \begin{bmatrix} x\cos\theta - y\sin\theta \\ x\sin\theta + y\cos\theta \end{bmatrix} \\ &= \underbrace{\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}}_{R_\theta} \begin{bmatrix} x \\ y \end{bmatrix}\end{aligned}$$

It is seen then that the rotation matrix rotates points in the xy-plane through an angle θ, or alternatively, it can be viewed as rotating the axes by $-\theta$.

(b) Show $R_\theta R_\mu = R_?$, $R_\theta^{-1} = R_?$.

Notice that

$$\begin{aligned} R_\theta R_\mu &= \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} \cos\mu & -\sin\mu \\ \sin\mu & \cos\mu \end{bmatrix} \\ &= \begin{bmatrix} \cos\theta\cos\mu - \sin\theta\sin\mu & -[\cos\theta\sin\mu + \sin\theta\cos\mu] \\ \sin\theta\cos\mu + \cos\theta\sin\mu & -\sin\theta\sin\mu + \cos\theta\cos\mu \end{bmatrix} \\ &= \begin{bmatrix} \cos(\theta+\mu) & -\sin(\theta+\mu) \\ \sin(\theta+\mu) & \cos(\theta+\mu) \end{bmatrix} = R_{\theta+\mu}, \end{aligned}$$

and

$$R_\theta R_{-\theta} = \begin{bmatrix} \cos(\theta-\theta) & -\sin(\theta-\theta) \\ \sin(\theta-\theta) & \cos(\theta-\theta) \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \mathbb{1},$$

meaning $R_\theta R_\mu = R_{\theta+\mu}$ and $R_\theta^{-1} = R_{-\theta}$.

(c) Let $G = \{R_\theta | \theta \in \mathbb{R}\}$. Show that G is a group under matrix multiplication.

<u>Proof</u>

Since the elements of G are matrices and matrix multiplication is associative, it follows that G is associative. We also see that R_0 is the identity element in G since it is also the 2×2 identity matrix. We showed in part (b) that $R_\theta^{-1} = R_{-\theta}$. It also suffices to show that $\det(R_\theta) = \cos^2\theta + \sin^2\theta = 1 \neq 0$, implying that each matrix in G has an inverse.

■

6[2.1.3]) Let $\mathbb{Z}$ denote the set of integers, and let

$$G = \{ \begin{bmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \Big| a \in \mathbb{Z}\}.$$

Prove that G together with the usual matrix multiplication forms a group.

Proof

Observe that G is associative since its elements are matrices and matrix multiplication is generally associative. Also, the element of G with $a = 1$ serves as the identity since

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & b & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & b & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

for any $b \in \mathbb{Z}$. Finally, we see that

$$\begin{vmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{vmatrix} = 1,$$

so every matrix in G has a unique inverse.

$\blacksquare$

7[2.2.1]) Let G be a group. Prove that $(ab)^{-1} = a^{-1}b^{-1}$ for all a and b in G if and only if G is abelian.

Proof

($\Leftarrow$) We have proven that $(ab)^{-1} = b^{-1}a^{-1}$ for any group. If G is abelian, then it follows that $b^{-1}a^{-1} = a^{-1}b^{-1}$.

($\Rightarrow$) Suppose that $(ab)^{-1} = a^{-1}b^{-1}$. We have also proven that $(ab)^{-1} = b^{-1}a^{-1}$. Hence, $(ab)^{-1} = (ba)^{-1}$ for all $a, b \in G$. This implies that $ab = ba$ (since each element has a unique inverse) and that G is abelian.

$\blacksquare$

8[2.2.2]) Let G be a group. Show that, for all $a, b \in G$, we have $(ab)^2 = a^2b^2$ if and only if G is abelian.

Proof

($\Leftarrow$) Let G be an abelian group. Then $ab = ba$ for all $a, b \in G$, and $(ab)^2 = abab = aabb = a^2b^2$.

($\Rightarrow$) Assume for all $a, b \in G$ that $(ab)^2 = a^2b^2$. Then $abab = aabb$. Multiplying on the left by a^{-1} and on the right by b^{-1} we have $a^{-1}(abab)b^{-1} = ba$ and $a^{-1}(aabb)b^{-1} = ab$. That is, $ba = ab$ or G is abelian.

$\blacksquare$

9[2.2.3]) If G is a group in which $a^2 = \mathbb{1}$ for all $a \in G$, show that G is abelian.

<u>Proof</u>

Observe that each element in G is its own inverse. That is $a = a^{-1}$. Thus, $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$, proving that G is abelian.

$\blacksquare$

10[2.2.4])

(a) If G is a finite group of even order, show that there must be an element $a \neq \mathbb{1}$, such that $a^{-1} = a$.

<u>Proof</u>

Since G is finite and even we have $G = \{\mathbb{1}, a_2, a_3, \dots, a_n\}$ where n is even. Suppose that for each element $a \neq \mathbb{1}$ that $a^{-1} \neq a$. However, there are $n-1$ elements which are not the identity, and since $2 \nmid n-1$, it is impossible that each element has a unique inverse. Thus, it must be the case that there exists at least one $a \neq \mathbb{1}$ in G such that $a^{-1} = a$.

$\blacksquare$

(b) Give an example to show that the conclusion of part (a) does not hold for groups of odd order.

$\rightarrow$ Consider a cyclic group of order 3: $\{\mathbb{1}, a, a^2\}$. It is clear that $a^{-1} = a^2$ and $(a^2)^{-1} = a$. As a concrete example consider $(\mathbb{Z}/5\mathbb{Z})^{\times}$ and $\langle \overline{2} \rangle = \{\overline{2}, \overline{4}, \overline{1}\}$. This is a group of order three with $\overline{1}^{-1} = \overline{1}$, $\overline{2}^{-1} = \overline{4}$, and $\overline{4}^{-1} = \overline{2}$.