1. (19 points) (a) $G$ is a set closed under a binary operation $\ast$. What three properties make $\langle G, \ast \rangle$ a group? Include the definitions of the terms used.

   i) **Associativity**: $\forall a, b, c \in G \ (a \ast b) \ast c = a \ast (b \ast c)$

   ii) **Identity**: $\exists e \in G \text{ such that } a \ast e = a = e \ast a \ \forall a \in G$

   iii) **Inverses**: For each $a \in G$, $\exists a^{-1} \in G \text{ such that } a \ast a^{-1} = e = a^{-1} \ast a$.

(b) The set $\mathbb{Z}$ is closed under the binary operation

\[ a \ast b = 4 + a + b. \]

Prove that $\langle \mathbb{Z}, \ast \rangle$ is a group.

   i) $(a \ast b) \ast c = (4 + a + b) \ast c = 4 + (4 + a + b) + c = 8 + a + b + c$

   ii) $a \ast e = a = e \ast a \iff 4 + a + e = a \iff e = -4$

   iii) $a \ast a^{-1} = e = a^{-1} \ast a \iff 4 + a + a^{-1} = -4$

So for $a \in \mathbb{Z}$, $a^{-1} = -a - 8 \in \mathbb{Z}$ is its inverse.
2. (12 points) (a) What two properties (or one property!) must be checked to show that a subset $H$ of a group $G$ is a subgroup?

i) $a, b \in H \Rightarrow ab \in H$

ii) $a \in H \Rightarrow a^{-1} \in H$

(b) Show that

$$H = \left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} : a \in \mathbb{Z} \right\}$$

is a subgroup of $M_2^+(\mathbb{R})$ (the $2 \times 2$ invertible matrices with real entries under matrix multiplication).

Note: $H$ is non-empty $\because [1, 0] \in H$

$A, B \in H \Rightarrow A = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \Rightarrow a, b \in \mathbb{Z}$

$A = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix} \in H \quad \text{since} \quad a+b \in \mathbb{Z}$

$A^{-1} = \begin{bmatrix} 1 & -a \\ 0 & 1 \end{bmatrix} \in H \quad \text{since} \quad -a \in \mathbb{Z}$.

3. (9 points) $G = \{e, a, b, c\}$ is a group of order 4 with identity $e$. A student has partially filled in the group table. Complete it or explain why this is not possible.

<table>
<thead>
<tr>
<th></th>
<th>e</th>
<th>a</th>
<th>b</th>
<th>c</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>a</td>
<td>b</td>
<td>c</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>e</td>
<td>c</td>
<td>b</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>c</td>
<td>e</td>
<td>a</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>b</td>
<td>a</td>
<td>e</td>
</tr>
</tbody>
</table>

$e \times e = e$  
$e \times e = e$

Since $G$ is a group each element appears exactly once in each row and each column.

4. (12 points) Short answer (no need to show your work!)

(a) In the group $\mathbb{Z}_3 \times \mathbb{Z}_6$ the inverse of $(2, 3)$ is $(1, 2)$

$$-(2, 3) = (-2, -3) \quad -2 = 1 \cdot 2 \in \mathbb{Z}_3$$

(b) In a group $G$ the equation $axb = c$ has the unique solution $x = a^{-1} c b^{-1}$.

(c) The order of the symmetric group $S_5$ is $5!$.

(d) In $\langle C^* \rangle$ the subgroup generated by $i = \sqrt{-1}$ is $\langle i \rangle = \{1, i, -1, -i\}$.

$$1, i, -i, -1, i, i^2, i^3, i^4 = 1$$
5. (10 points) For the permutations in $S_9$

$$\sigma = (1\ 3\ 5\ 7) (2\ 4\ 8) (6\ 9), \quad \tau = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9)$$

(a) What is the order of $\sigma$?

$$\sigma = (1\ 3\ 5\ 7) (2\ 4\ 8) (6\ 9) \quad \text{ord}(\sigma) = \text{lcm}(4, 3, 2) = 12$$

(b) Write $\sigma \tau^{-1}$ as a product of disjoint cycles.

$$\sigma \tau^{-1} = (1\ 2\ 7\ 9) (3) (4\ 5\ 6\) (8) = (1279)(456)$$

6. (12 points) Let $G$ be a group. For a fixed element $g$ in $G$ define $\phi : G \to G$ by

$$\phi(x) = gxg^{-1}.$$ 

(i) Show that $\phi$ is surjective.

Suppose $y \in G$. We need to show $\exists x \in G$ s.t. $\phi(x) = y$.

$$gxg^{-1} = y \implies x = g^{-1}yg \in G$$

$$\phi(g^{-1}yg) = \phi(g^{-1}yg)g^{-1}$$

$$= (g^{-1})yg(g^{-1})$$

$$= e \neq e$$

$$= y$$

(ii) Show that $\phi$ is injective.

Suppose $\phi(x_1) = \phi(x_2)$, $x_1, x_2 \in G$. We need to show that $x_1 = x_2$.

$$gx_1g^{-1} = gx_2g^{-1}$$

$$\sigma^{-1}(gx_1g^{-1})g = \sigma^{-1}(gx_2g^{-1})g \quad \{\text{or use cancellation law on left and right}\}$$

$$(\sigma^{-1}g)x_1(\sigma^{-1}g) = (\sigma^{-1}g)x_2(\sigma^{-1}g)$$

$$e \cdot e = e \cdot e$$

$$x_1 = x_2$$
7. (16 points) Circle True (T) or False (F).

T (F) (a) \( a \times b = a - b \) is a commutative binary operation on \( \mathbb{Z} \).

T (F) (b) \( a \times b = a - b \) is an associative binary operation on \( \mathbb{Z} \).

T (F) (c) The set \( \left\{ \begin{pmatrix} a & 0 \\ 0 & 2a \end{pmatrix} : a \in \mathbb{R}^+ \right\} \) is closed under matrix multiplication.

T (F) (d) \( S = \{ (a, 3a) : a \in \mathbb{Q} \} \) forms a subgroup of \( \mathbb{R} \times \mathbb{R} \).

T (F) (e) \( < \mathbb{Z}, + > \) is a cyclic group.

T (F) (f) \( \left\{ \begin{pmatrix} a \\ 0 \\ 0 \\ a \end{pmatrix} : a \in \mathbb{R}^+ \right\} \) has no identity under matrix multiplication.

T (F) (g) \( < \mathbb{Q}^{\text{pos}}, \cdot > \) is a group.

T (F) (h) \( < \mathbb{Q}^{\ast}, \div > \) is a group.

\[ \div \text{ is not associative} \]

\[ (a \div b) \div c = a \div (b \div c) \]

8. (10 points) Let \( < G, \ast > \) be a group and let \( a \) be a fixed element of \( G \). Define

\[ S = \{ x \in G \mid x \ast a = a \ast x \} \].

(i) Prove that \( S \) is closed under \( \ast \).

\[
\begin{align*}
\text{Suppose } & x, y \in S \quad \text{is } \quad x \ast a = a \ast x \quad \text{and} \quad y \ast a = a \ast y \quad \text{we need to show } \quad xy \ast a = a \ast (xy) \quad (\text{we need to show } \quad xy \in S) \\
(x \ast y) \ast a & = x \ast (y \ast a) \quad \text{Assoc.} \\
& = x \ast (a \ast y) \quad \text{YES} \\
& = (x \ast a) \ast y \quad \text{Assoc.} \\
& = (a \ast x) \ast y \quad \text{YES} \\
& = a \ast (x \ast y) \quad \text{Assoc.} \quad \text{so } x \ast y \in S
\end{align*}
\]

(ii) Prove that \( S \) is a subgroup of \( G \).

\[
\begin{align*}
S \text{ is non-empty!} \quad \text{e} \ast a = a \Rightarrow e \ast e \in S \\
\text{(i) Show closure so we just need to show inverses.} \\
\text{Suppose } z \in S \quad \text{is } \quad z \ast a = a \ast z \quad (\text{we need to show } \quad z^{-1} \in S) \\
\quad \text{So } x \ast (x \ast a) = a \ast (x \ast x^{-1}) \\
\quad \text{Def inverse} \\
\quad \text{Def identity} \\
\end{align*}
\]