Answers to Chapter 2 Exercises

**Exercise 3.** Show that \( \{1, 2, 3\} \) under multiplication modulo 4 is not a group but \( \{1, 2, 3, 4\} \) under multiplication modulo 5 is a group.

*Proof.* In the first situation, we note that \( 2 \times 2 = 0 \pmod{4} \) and that \( 0 \notin \{1, 2, 3\} \). Thus the binary operation is not closed. (Alternately, show that 2 does not have an inverse.)

In the second situation, we note that multiplication modulo \( n \) is associative for all \( n \). Clearly, 1 serves as the identity. And

\[
\begin{align*}
1 \times 1 &= 1 \pmod{5} \\
2 \times 3 &= 1 \pmod{5} \\
4 \times 4 &= 1 \pmod{5}
\end{align*}
\]

establishes the existence of inverses for each element. Ergo, the set and operation satisfy the definition of group. \( \square \)

**Exercise 12.** For any integer \( n > 2 \), show that there are at least two elements in \( U(n) \) that satisfy \( x^2 = 1 \).

*Proof.* We begin by showing that two elements exist in \( U(n) \), namely 1 and \( n - 1 \). Clearly, \( \gcd(n, 1) = 1 \) for all \( n \) since 1 is its only divisor. Using the Euclidean Algorithm, we see that

\[
\gcd(n, n - 1) = \gcd(n \mod n - 1, n - 1) = \gcd(1, n - 1) = 1.
\]

Thus, \( (n - 1) \in U(n) \), and for \( n > 2 \), \( n - 1 \) is distinct from 1.

Now we observe the following:

\[
1^2 = 1 \pmod{n}
\]

and

\[
(n - 1)^2 = n^2 - 2n + 1 = 0 - 0 + 1 = 1 \pmod{n}
\]

Thus, at least two elements of \( U(n) \) satisfy the given equation. \( \square \)

**Exercise 25.** Suppose the table below is a group table. Fill in the blank entries.

*Solution.* We will make use of the identity element \( e \) to fill in the first row and first column. We then use the Latin square property noted in Exercise 23 to complete row and columns that have one blank.

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