Assigned reading: Chapters 1-3 of Gallian.

Recommended practice questions: Chapter 1 of Gallian, exercises 1, 2, 4, 5, 6, 7, 11
Chapter 2 of Gallian, exercises 17, 31, 33, 34, 44, 46, 47, 48, 49
Chapter 3 of Gallian, exercises 1, 7

Assigned questions to hand in:

(1) (Gallian Chapter 1 # 13) Describe the symmetries of a nonsquare rectangle. Construct the corresponding Cayley (multiplication) table.

Solution:

<table>
<thead>
<tr>
<th>Identity: $e$</th>
<th>Flip over vertical: $F_v$</th>
<th>Flip over horizontal: $F_h$</th>
<th>Rotate 180°: $R_{180}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 2</td>
<td>3 4</td>
<td>1 2</td>
<td>3 4</td>
</tr>
</tbody>
</table>

To compute the multiplication table, we notice that

$F_v \circ F_h = R_{180} = F_h \circ F_v$,

and

$F_v \circ R_{180} = F_h,$  $F_h \circ R_{180} = F_v,$  etc.

Thus,

<table>
<thead>
<tr>
<th>$\circ$</th>
<th>$e$</th>
<th>$F_v$</th>
<th>$F_h$</th>
<th>$R_{180}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e$</td>
<td>$e$</td>
<td>$F_v$</td>
<td>$F_h$</td>
<td>$R_{180}$</td>
</tr>
<tr>
<td>$F_v$</td>
<td>$F_v$</td>
<td>$e$</td>
<td>$R_{180}$</td>
<td>$F_h$</td>
</tr>
<tr>
<td>$F_h$</td>
<td>$F_h$</td>
<td>$R_{180}$</td>
<td>$e$</td>
<td>$F_v$</td>
</tr>
<tr>
<td>$R_{180}$</td>
<td>$R_{180}$</td>
<td>$F_h$</td>
<td>$F_v$</td>
<td>$e$</td>
</tr>
</tbody>
</table>

(2) (Gallian Chapter 2 # 18) List the members of $H = \{x^2 : x \in D_4\}$ and $K = \{x \in D_4 : x^2 = e\}$.

Solution: Recall that

$D_4 = \{e, R_{90}, R_{180}, R_{270}, F, FR_{90}, FR_{180}, FR_{270}\}$. 
Also note that \( R_{90}F = FR_{270} \) and \( R_{180}F = FR_{180} \). We compute the square of each element in \( D_4 \).

\[
\begin{align*}
  e^2 &= e & F^2 &= e \\
  R_{90}^2 &= R_{180} & (FR_{90})^2 &= FFR_{270}R_{90} = e \\
  R_{180}^2 &= R_{360} = e & (FR_{180})^2 &= FFR_{180}R_{180} = e \\
  R_{270}^2 &= R_{540} = R_{180} & (FR_{270})^2 &= FFR_{90}R_{270} = e.
\end{align*}
\]

Thus, the elements of \( D_4 \) that can be written as squares of other elements are

\[
  H = \{e, R_{180}\}.
\]

And, the set of idempotent elements of \( D_4 \) (elements that square to the identity) are

\[
  K = \{e, R_{180}, F, FR_{90}, FR_{180}, FR_{270}\}.
\]

(3) (Gallian Chapter 2 # 32) Construct a Cayley (multiplication) table for \( U(12) \).

Solution: By definition,

\[
  U(12) = \{a \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\} : gcd(a, 12) = 1\}
  = \{1, 5, 7, 11\}.
\]

The multiplication table is

\[
  \begin{array}{c|cccc}
    \times_{12} & 1 & 5 & 7 & 11 \\
    \hline
    1 & 1 & 5 & 7 & 11 \\
    5 & 5 & 1 & 11 & 7 \\
    7 & 7 & 11 & 1 & 5 \\
    11 & 11 & 7 & 5 & 1
  \end{array}
\]

(4) (Gallian Chapter 2 # 36) Let \( a, b \) belong to a group \( G \). Find an \( x \) in \( G \) such that \( xabx^{-1} = ba \).

Solution: Let \( x = b \). Then

\[
  bab^{-1} = ba(bb^{-1}) = bae = ba.
\]

(5) (Gallian Chapter 3 # 4) Prove that in any group, an element and its inverse have the same order.

Solution: Recall the definition (p. 60) that the order of an element \( g \) of a group is the smallest positive integer \( n \) such that \( g^n = e \). First, we will prove that \( |g^{-1}| \leq |g| \). To do so, let \( n = |g| \). Then

\[
  (g^{-1})^n = g^{-n} = (g^n)^{-1} = e^{-1} = e.
\]

Since \( |g^{-1}| \) is the smallest positive number with this property, we have \( |g^{-1}| \leq n = |g| \), as required.

To finish the proof, recall that the inverse of \( g^{-1} \) is \( g \). Therefore, by the above argument,

\[
  |g| = |(g^{-1})^{-1}| \leq |g^{-1}|.
\]

We have proved that \( |g^{-1}| \leq |g| \) and \( |g| \leq |g^{-1}| \), thus, \( |g| = |g^{-1}| \).
(6) (Gallian Chapter 3 # 6) In the group $\mathbb{Z}_{12}$, find $|a|$, $|b|$, and $|a + b|$ for each case.

(a) $a = 6$, $b = 2$
(b) $a = 3$, $b = 8$
(c) $a = 5$, $b = 4$
Do you see any relationship between $|a|$, $|b|$, and $|a + b|$?

Solution:
(a) For $a$:
$$1 \cdot 6 \mod 12 \neq 0, \quad 2 \cdot 6 \mod 12 = 6 + 6 \mod 12 = 12 \mod 12 = 0$$
so $|6| = 2$. For $b$:
$$1 \cdot 2 \mod 12 \neq 0, \quad 2 \cdot 2 \mod 12 \neq 0, \quad 3 \cdot 2 \mod 12 \neq 0,$$
$$4 \cdot 2 \mod 12 \neq 0, \quad 5 \cdot 2 \mod 12 \neq 0, \quad 6 \cdot 2 \mod 12 = 0$$
so $|2| = 6$. For $a + b$:
$$1 \cdot 8 \mod 12 \neq 0, \quad 2 \cdot 8 \mod 12 \neq 0, \quad 3 \cdot 8 \mod 12 = 0$$
so $|6 + 2| = 3$.

(b) For $a$:
$$1 \cdot 3 \mod 12 \neq 0, \quad 2 \cdot 3 \mod 12 = 0, \quad 3 \cdot 3 \mod 12 \neq 0, \quad 4 \cdot 3 \mod 12 = 0$$
so $|3| = 4$. For $b$, our work in part (a) gives $|8| = 3$. For $a + b$:
$$1 \cdot 11 \mod 12 \neq 0, \quad 2 \cdot 11 \mod 12 \neq 0, \quad 3 \cdot 11 \mod 12 = 0$$
$$4 \cdot 11 \mod 12 \neq 0, \quad 5 \cdot 11 \mod 12 \neq 0, \quad 6 \cdot 11 \mod 12 = 0$$
$$7 \cdot 11 \mod 12 \neq 0, \quad 8 \cdot 11 \mod 12 \neq 0, \quad 9 \cdot 11 \mod 12 = 0$$
$$10 \cdot 11 \mod 12 \neq 0, \quad 11 \cdot 11 \mod 12 \neq 0, \quad 12 \cdot 11 \mod 12 = 0$$
so $|3 + 8| = 12$.

(c) For $a$:
$$1 \cdot 5 \mod 12 \neq 0, \quad 2 \cdot 5 \mod 12 \neq 0, \quad 3 \cdot 5 \mod 12 \neq 0$$
$$4 \cdot 5 \mod 12 \neq 0, \quad 5 \cdot 5 \mod 12 \neq 0, \quad 6 \cdot 5 \mod 12 \neq 0$$
$$7 \cdot 5 \mod 12 \neq 0, \quad 8 \cdot 5 \mod 12 \neq 0, \quad 9 \cdot 5 \mod 12 \neq 0$$
$$10 \cdot 5 \mod 12 \neq 0, \quad 11 \cdot 5 \mod 12 \neq 0, \quad 12 \cdot 5 \mod 12 = 0$$
so $|5| = 12$. For $b$:
$$1 \cdot 4 \mod 12 \neq 0, \quad 2 \cdot 4 \mod 12 \neq 0, \quad 3 \cdot 4 \mod 12 = 0,$$
so $|4| = 3$. For $a + b$:
$$1 \cdot 9 \mod 12 \neq 0, \quad 2 \cdot 9 \mod 12 \neq 0, \quad 3 \cdot 9 \mod 12 \neq 0, \quad 4 \cdot 9 \mod 12 = 0$$
so $|5 + 4| = 4$. 

3
(7) (Gallian Chapter 3 # 32) If $H$ and $K$ are subgroups of $G$, show that $H \cap K$ is a subgroup of $G$. (Can you see that the same proof shows that the intersection of any number of subgroups of $G$, finite or infinite, is again a subgroup of $G$?)

Solution: Assume $H$ and $K$ are subgroups of $G$. In particular, this implies that $e \in H$ and $e \in K$. Using Theorem 3.1, it is enough to prove that $H \cap K$ is nonempty and that if $a, b \in H \cap K$ then $ab^{-1} \in H \cap K$. First, observe that $e \in H \cap K$ (because by assumption it is in each of these sets) and hence $H \cap K$ is nonempty. Now, let $a, b \in H \cap K$. Then $a, b \in H$ and $a, b \in K$. Since $H$ is a group (and hence closed under the operation and inverses), $ab^{-1} \in H$. Symmetrically, $ab^{-1} \in K$. Thus, $ab^{-1} \in H \cap K$, as required.