The exam is 150 minutes long and worth a total of 100 points. No books, notes or calculators may be used. **Show all of your work and justify your answers carefully.** You will be graded on the clarity of your exposition as well as the correctness of your answers.

*Good luck.*

UBC Rules governing examinations:

(a) Each candidate should be prepared to produce his/her UBCcard upon request for identification.

(b) Candidates are not permitted to ask questions of the invigilators, except in cases of supposed errors or ambiguities in the examination questions.

(c) No candidate shall be permitted to enter the examination room after the expiration of one half hour from the scheduled starting time, or to leave during the first half hour, or the last 15 minutes of the examination.

(d) Candidates guilty of any of the following or similar dishonest practices shall be immediately dismissed from the examination, and shall be liable to disciplinary action:
   a) Making use of any books, papers or memoranda, calculators, computers, sound or image players/recorders/transmitters (including phones), or other memory aid devices other than those authorized by the examiners.
   b) Speaking or communicating with other candidates.
   c) Purposely exposing written papers to the view of other candidates or imaging devices. The plea of accident or forgetfulness will not be received.

(e) Candidates must not destroy or mutilate any examination material; must hand in all examination papers; and must not take any examination material from the examination room without permission of the invigilator.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td></td>
</tr>
</tbody>
</table>
1 (10 points). *Inverse elements:* Calculate the inverse of the following elements in $\mathbb{Z}/18\mathbb{Z}$.

(a) $[11]_{18}$
(b) $[7]_{18}$
(c) $[15]_{18}$
2 (10 points). Group theory: The following set of 2 × 2 matrices

\[ m_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad m_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad m_3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \quad m_4 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \]

\[ m_5 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad m_6 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad m_7 = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \quad m_8 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \]

with matrix multiplication forms a group, \(G\).

(a) (2 points) List the elements of its subgroup, \(K\), generated by the element \(\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\).

(b) (8 points) Compute the left cosets of \(K\).
3 (15 points). Error detecting code ISBN-13: Consider the 10-ary code of length 13, using the alphabet $\mathbb{Z}/10\mathbb{Z}$ and following encoding algorithm.

ENCODE: $x_1x_2\cdots x_{12} \mapsto x_1x_2\cdots x_{12}x_{13}$ by

$$\sum_{i \text{ odd}} x_i + \sum_{i \text{ even}} 3x_i \equiv 0 \pmod{10}.$$ 

Answer the following questions.

(a) (7 points) Find the missing digit of the ISBN-13 that is 97803 ? 6406156.

(b) (8 points) Explain why this code can detect one error.
Coding theory:

(a) (6 points) Show that the following two 4-ary non-linear codes are equivalent
\[ C = \{0122, 1033, 2303, 3210\} \quad C' = \{0220, 1331, 2001, 3113\}. \]

(b) (9 points) Show that a q-ary \(((q + 1), M, 3)\) code satisfies \( M \leq q^{q-1} \).
5 (15 points). Linear codes: Consider the 3-ary linear code, $C$, with parity check matrix 
\[
\begin{pmatrix}
1 & 2 & 1
\end{pmatrix}.
\]

(a) (10 points) List all the codewords in $C$. Determine how many errors $C$ can detect.

(b) (5 points) Let $D$ be the binary linear code with parity check matrix 
\[
\begin{pmatrix}
1 & 1 & 0 \\
1 & 0 & 1
\end{pmatrix}.
\]

Compute the coset leaders of $D$. 
6 (15 points). Order of an element:

(a) (5 points) Define the order of a unit in a ring.

(b) (10 points) Given the ring \( \mathbb{Z}/m\mathbb{Z} \), prove that

\[
\text{if } e \text{ is the order of a unit } [a]_m \in \mathbb{Z}/m\mathbb{Z} \text{ and } [a]^f = [1]_m \text{ then } e \mid f.
\]