1 (To be handed in). In class, we looked at a three-way system for transferring a message from A to B, which had the interesting property that neither A nor B had to reveal their keys. Given a message \( m \), the first message (from A to B) would be \( K_A(m) \), the second message (from B to A) would be \( K_B(K_A(m)) \), and the third message (from A to B) would be \( K_A^{-1}(K_B(K_A(m))) = K_B(m) \). B could then calculate \( K_B^{-1}(K_b(m)) = m \), and retrieve the message. If both A to B used a random byte sequence for their key, and then used the XOR function to both encrypt and decrypt the message, then surely this is a perfect technique for transferring data... right? (Neither participant has to reveal a key, and a third party cannot decrypt/unlock the message).

Well... actually... it is not a good scheme. Explain exactly why it is not a good scheme.

Please come to the tutorial ready to present your answers to these questions as well:

2 (Do not hand in). Fields and Groups:

(a) Why are the Integers using addition and multiplication not a field?
(b) Why are the Natural numbers using addition not a group?
(c) Show the tables for addition and multiplication for the positive integers mod 5 (\( Z_5 \)) similar to the table on page 23 of the book.

3 (Do not hand in). Fields and Groups:

(a) Consider the table below, Hugh’s loony three-valued logic. Does \( \{\circ, \perp, \top, \nabla\} \) form a group? If so, what is the \( \nabla \) identity?

<table>
<thead>
<tr>
<th></th>
<th>( \circ )</th>
<th>( \nabla )</th>
<th>( \top )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \nabla )</td>
<td>( \perp )</td>
<td>( \circ )</td>
<td>( \perp )</td>
</tr>
<tr>
<td>( \top )</td>
<td>( \perp )</td>
<td>( \top )</td>
<td>( \nabla )</td>
</tr>
</tbody>
</table>

(b) The other operator for loony logic is given below. Does \( \{\circ, \perp, \top, \nabla, \Delta\} \) form a field? If so, prove it by renaming and properties of fields.

<table>
<thead>
<tr>
<th></th>
<th>( \circ )</th>
<th>( \perp )</th>
<th>( \top )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \Delta )</td>
<td>( \circ )</td>
<td>( \perp )</td>
<td>( \top )</td>
</tr>
<tr>
<td>( \nabla )</td>
<td>( \perp )</td>
<td>( \top )</td>
<td>( \nabla )</td>
</tr>
<tr>
<td>( \perp )</td>
<td>( \nabla )</td>
<td>( \perp )</td>
<td>( \perp )</td>
</tr>
<tr>
<td>( \top )</td>
<td>( \perp )</td>
<td>( \top )</td>
<td>( \nabla )</td>
</tr>
</tbody>
</table>

4 (Do not hand in). Describe an operation \( \bullet \) which forms a group with the Integers from 3 to 6. Define the operation, and give the identity, and the inverse mappings.