Homework 12

Question from text

\{0, 1, 2, 3\} with \(+_\text{Mod4}\) as a group.

\[
\begin{array}{c|cccc}
+ & 0 & 1 & 2 & 3 \\
\hline
0 & 0 & 1 & 2 & 3 \\
1 & 1 & 2 & 3 & 0 \\
2 & 2 & 3 & 0 & 1 \\
3 & 3 & 0 & 1 & 2 \\
\end{array}
\]

\(\text{G1}\) The operation \(+\) is a function, and the set \(\{0, 1, 2, 3\}\) is closed under \(+\).

\(\text{G2}\) \(+\) is associative – easily checked in the table.

\(\text{G3}\) 0 is the identity element.

\(\text{G4}\) \(0 + 0 = 0\) \(1 + 3 = 0\) \(2 + 2 = 0\) \(3 + 1 = 0\)

Therefore, clearly every element in the carrier has an inverse.

Question 2

Show that no Boolean Algebra can be a group.

I will show this by assuming that a Boolean Algebra that is also a group does exist, and then deducing a contradiction from the axioms for Groups and Boolean Algebras. References to axioms are to Boolean Algebra and Group axioms in PtMW (p. 295, 255).

[1] Let \(\text{BG}\) be a Boolean Algebra in the signature \(\Omega = \{0, 1, \ast, \lor, \land\}\), that is also a Group with respect to one of its operations.

We will now consider each of the two binary operations \((\lor, \land)\) in turn.

[2] Consider first the operation \(\lor\).

For all \(a \in \text{BG}\), \(a \lor 0 = a\) \hspace{1cm} (B5)

\(\therefore\) 0 is the identity element for \(\lor\).

[3] For all \(a \in \text{BG}\), there is some \(x\) such that:

\(a \lor x = 0\) \hspace{1cm} (G4)

\(\therefore\) Every element of \(\text{BG}\) has an inverse with respect to \(\lor\).

[4] For all \(x \in \text{BG}\), \(x \lor 1 = 1\). \hspace{1cm} (B5)

[5] For all \(x \in \text{BG}\), \(1 \lor x = 1\). \hspace{1cm} \[4\] and \(\text{(B1)}\)
There is some $x \in BG$, such that $1 \lor x = 0$. \[3\]


Now consider the other binary operation, $\land$.

For all $b \in BG$, $b \land 1 = b$. \[B5\]

$\therefore$ 1 is the identity element for $\land$.

For all $b \in BG$, there is some $y$ such that:

$b \land y = 1$. \[G4\]

$\therefore$ Every element of $BG$ has an inverse with respect to $\land$.

For all $y \in BG$, $y \land 0 = 0$. \[B5\]

For all $y \in BG$, $0 \land y = 0$. \[10\] and \[B1\] (Associativity)

There is some $y \in BG$, such that $0 \land y = 1$. \[9\]


Therefore, for both binary operations of $BG$, we derive a contradiction. Therefore $BG$ cannot be both a Boolean Algebra and a Group.

[Instructor’s note: But one-element Boolean Algebra is a Group.]

**Question 3: PtMW, p. 272, Question 5**

(a) Below is the multiplication table Mod6, without $\{0\}$:

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

This is not a group. The first axiom for being a group, is that the system must be an algebra. And this is not an algebra, because the set $\{1, 2, 3, 4, 5\}$ is not closed under $\times_{\text{Mod6}}$. It is not closed under this operation, because we have 0 as the result of the operation on several members of the set $\{1, 2, 3, 4, 5\}$, but 0 is not in this set itself.
(b) Below is the multiplication table Mod7, without \{0\}:

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>1</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>6</td>
<td>2</td>
<td>5</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>1</td>
<td>5</td>
<td>2</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

(G1) The set \{1, 2, 3, 4, 5, 6\} is closed under $\times_{\text{Mod7}}$, and the operation $\times_{\text{Mod7}}$ applied to two members of the set always gives the same result. Therefore, this system is an algebra.

(G2) It is laborious to check, but the operation is $\times_{\text{Mod7}}$ indeed associative. But, we also know that multiplication is associative.

(G3) There is an identity element, namely 1.

(G4) Every element does have an inverse:

<table>
<thead>
<tr>
<th>Element</th>
<th>Inverse</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
</tr>
</tbody>
</table>

(c) Let the group defined in (b) above be \(G\). Any subgroup of \(G\) will have to include the identity element 1. Therefore, one trivial subgroup is \(\{1\}\) with $\times_{\text{Mod7}}$.

If we add any other members from the original set \(G\), we will always have to add both the member and its inverse. Since multiplication is commutative, an element will always be the inverse of its inverse. Therefore, adding both an element and its inverse, will still result in a set that is closed under $\times_{\text{Mod7}}$.

Therefore any subset \(G'\) of \(G = \{1, 2, 3, 4, 5, 6\}\) with the operation $\times_{\text{Mod7}}$ defined on it, will be a subgroup \(G\) if it satisfies the following two conditions:

(i) $1 \in G'$

(ii) $\forall x (x \in G' \rightarrow \exists y (y \in G' \& (x \times_{\text{Mod7}} y = 1))$

Therefore, all of the following subsets are with defined on them, will therefore be subgroups of \(G\): \(\{1\}\), \(\{1, 2, 4\}\), \(\{1, 3, 5\}\), \(\{1, 6\}\), \(\{1, 2, 4, 3, 5\}\), \(\{1, 2, 4, 6\}\), \(\{1, 3, 5, 6\}\).
**Question 4: PtMW p. 273, Question 9**

\[ A = \{a, b\} \quad \mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\} \]

Consider first the operation \( \cup \). Let us call this system **Union**. We can define the following operation table for \( \cup \):

\[
\begin{array}{c|c|c|c|c}
\emptyset & \emptyset & \{a\} & \{b\} & \{a, b\} \\
\hline
\{a\} & \{a\} & \{a\} & \{a, b\} & \{a, b\} \\
\hline
\{b\} & \{b\} & \{a, b\} & \{b\} & \{a, b\} \\
\hline
\{a, b\} & \{a, b\} & \{a, b\} & \{a, b\} & \{a, b\} \\
\end{array}
\]

(G1) **Union** is an algebra – the carrier of **Union**, \( \mathcal{P}(A) \), is closed under the operation \( \cup \), and \( \cup \) is a function.

(G2) We know that set union is associative.

(G3) \( \emptyset \) is the identity element.

(G4) But only \( \emptyset \) has an inverse, namely itself.

Conclusion: By Satisfying (G1) and (G2), **Union** qualifies as a semigroup. However, since it doesn’t satisfy (G4), it is not a group.

Now consider the operation \( \cap \). Let us call this system **Intersect**. We can define the following operation table for \( \cap \):

\[
\begin{array}{c|c|c|c|c}
\emptyset & \emptyset & \{a\} & \{b\} & \{a, b\} \\
\hline
\{a\} & \emptyset & \{a\} & \emptyset & \emptyset \\
\hline
\{b\} & \{a\} & \emptyset & \{a\} & \{a\} \\
\hline
\{a, b\} & \emptyset & \emptyset & \{b\} & \{b\} \\
\end{array}
\]

(G1) **Intersect** is an algebra – the carrier of **Intersect**, \( \mathcal{P}(A) \), is closed under the operation \( \cap \), and \( \cap \) is a function.

(G2) We know that set intersection is associative.

(G3) \{a, b\} is the identity element.

(G4) But only \{a, b\} has an inverse.

Conclusion: By Satisfying (G1) and (G2), **Intersect** qualifies as a semigroup. However, since it doesn’t satisfy (G4), it is not a group.

The following it is true of both **Union** and **Intersect** that: (i) the carrier is has a cardinality 4, (ii) there is a single binary operation that is associative, (ii) there is an
identity element, (iii) only the identity element has an inverse. Since this is true of both semigroups, setting up an isomorphism between them is trivially easy.

Let \( i: \mathcal{P}(A) \to \mathcal{P}(A) \), defined as follows:

\[
\begin{align*}
i(\emptyset) &= \{a, b\} \\
i(\{a, b\}) &= \emptyset \\
i(\{a\}) &= \{a\} \\
i(\{b\}) &= \{b\}
\end{align*}
\]

And let \( \cup \) correspond to \( \emptyset \).

Then \( i \) is an isomorphism between **Union** and **Intersect**. I will show this by rearranging the operation table for **Intersect** to correspond to that of **Union**. Comparing the two operation tables will then make it clear that they have the exact same structure. Since the size of the operation tables are equal and they have the same structure, the two algebras are isomorphic.

\[
\begin{array}{c|c|c|c|c}
\emptyset & \{a, b\} & \{a\} & \{b\} & \emptyset \\
\hline
\{a, b\} & \{a, b\} & \{a\} & \{b\} & \emptyset \\
\{a\} & \{a\} & \{a\} & \emptyset & \emptyset \\
\{b\} & \{b\} & \emptyset & \{b\} & \emptyset \\
\hline
\emptyset & \emptyset & \emptyset & \emptyset & \emptyset
\end{array}
\]

\[
\begin{array}{c|c|c|c|c|c}
\emptyset & \emptyset & \{a\} & \{b\} & \{a, b\} \\
\hline
\emptyset & \emptyset & \{a\} & \{b\} & \{a, b\} \\
\{a\} & \{a\} & \{a\} & \{a, b\} & \{a, b\} \\
\{b\} & \{b\} & \{a, b\} & \{b\} & \{a, b\} \\
\{a, b\} & \{a, b\} & \{a, b\} & \{a, b\} & \{a, b\}
\end{array}
\]
(a) To prove: $a^m \circ a^n = a^{m+n}$

Or alternatively, for all $n \in D$, $P(n) = a^m \circ a^n = a^{m+n}$. Then we have to prove $P(n)$ for all $n \in D$.

We will assume that in an integral domain $D$:

(A1) $a^1 = a$

(A2) $a^{n+1} = a^n \circ a$

**Step 1: The basis of the induction**

Let $n = 1$.

$a^m \circ a^n = a^m \circ a^1$

$a^m \circ a^1 = a^m \circ a$ (A1)

$a^m \circ a = a^{m+1}$ (A2)

$a^m \circ a^1 = a^{m+1}$

**Step 2: The recursive step**

Assume for an arbitrary $k \in D$ that $a^m \circ a^k = a^{m+k}$. Then:

$a^m \circ a^{k+1} = a^m \circ (a^k \circ a)$ (A2)

$a^m \circ (a^k \circ a) = (a^m \circ a^k) \circ a$ Assciativity.

$(a^m \circ a^k) \circ a = a^{m+k} \circ a$ By assumption.

$a^{m+k} \circ a = a^{m+k+1}$ (A2)

$a^m \circ a^{k+1} = a^{m+(k+1)}$

Therefore if $a^m \circ a^k = a^{m+k}$, then $a^m \circ a^{k+1} = a^{m+(k+1)}$

Or alternatively, if for an arbitrary $k$, if $P(k)$, then $P(k+1)$.

**Step 3: The conclusion**

We have shown that $P(n)$ for $n = 1$ [Step 1]. Since we have chosen an arbitrary $k$ in Step 2, it follows that $P(n)$ is true of all positive integers $n$. 

(b) To prove: \((a^m)^n = (a^n)^m\)

Or alternatively, for all \(n \in D\), \(P(n) = (a^m)^n = (a^n)^m\). Then we have to prove \(P(n)\) for all \(n \in D\).

We will assume that in an integral domain \(D\):

(A1) \[a^1 = a\]
(A2) \[a^{n+1} = a^n \circ a\]
(A3) \[a^n \circ b^n = (a \circ b)^n\]

**Step 1: The basis of the induction**

Let \(n = 1\).

\[(a^m)^1 = (a^m)^1\]
\[(a^m)^1 = a^m\] \hspace{1cm} (A1)
\[(a^m)^n = (a^1)^n\]
\[(a^1)^n = a^m\] \hspace{1cm} (A1)
\[(a^m)^1 = (a^1)^m\]

**Step 2: The recursive step**

Assume for an arbitrary \(k \in D\) that \((a^m)^k = (a^k)^m\). Then:

\[(a^m)^{k+1} = (a^m)^k \circ a^m\] \hspace{1cm} (A2)
\[(a^m)^k \circ a^m = (a^k)^m \circ a^m\] Assumed.
\[(a^k)^m \circ a^m = (a^k \circ a)^m\] \hspace{1cm} (A3)
\[(a^k \circ a)^m = (a^{k+1})^m\] \hspace{1cm} (A2)
\[(a^m)^{k+1} = (a^{k+1})^m\]

Therefore, if \((a^m)^k = (a^k)^m\), then \((a^m)^{k+1} = (a^{k+1})^m\).

Or alternatively, if for an arbitrary \(k\), if \(P(k)\), then \(P(k + 1)\).

**Step 3: The conclusion**

We have shown that \(P(n)\) for \(n = 1\) [Step 1]. Since we have chosen an arbitrary \(k\) in Step 2, it follows that \(P(n)\) is true of all positive integers \(n\).