MATH 31 – HOMEWORK 1 SOLUTIONS!

due Wednesday, July 5

Instructions: This assignment is due at the *beginning* of class. Staple your work together (do not just fold over the corner). Please write the questions in the correct order. If I cannot read your handwriting, you won't receive full credit.

---

1. (3.11) Let $(G, \star)$ be a group such that $x^2 = e$ for all $x \in G$. Show that $(G, \star)$ is abelian. (Here, x^2 is shorthand for $x \star x$.)

   Solution: There are many ways to prove this. Here's one. First notice that $x = x^{-1}$ for all $x \in G$ (i.e., every element is its own inverse). This is because $x \star x = e$. Now let x and y be arbitrary. Then,

   $$x \star y = (x \star y)^{-1} = y^{-1} \star x^{-1} = y \star x.$$

   The middle equality is a theorem from class. Since x and y were arbitrary, we've shown that $(G, \star)$ is abelian.

---

2. (3.12) Let $(G, \star)$ be a group. Show that $(G, \star)$ is abelian if and only if $(x \star y)^2 = x^2 \star y^2$ for all $x, y \in G$.

   Solution: Because this is an if and only if statement, there are two things to prove.

   For the first direction, ($\Longrightarrow$), suppose $(G, \star)$ is abelian. Then, we clearly see that

   $$(x \star y)^2 = (x \star y) \star (x \star y) = x \star y \star x \star y = x \star x \star y \star y = x^2 \star y^2.$$

   This completes the first direction.

   To prove the ($\Longleftarrow$) direction, let x and y be arbitrary. By assumption,

   $$(x \star y)^2 = x^2 \star y^2.$$

   Writing out both sides, this says

   $$x \star y \star x \star y = x \star x \star y \star y.$$

   Multiply both sides by x^{-1} on the left and y^{-1} on the right. The result is

   $$x^{-1} \star x \star y \star x \star y \star y^{-1} = x^{-1} \star x \star x \star y \star y \star y^{-1},$$

   and therefore

   $$y \star x = x \star y.$$

   Since x and y were arbitrary, G is abelian.

---

3. Let $G = \{5, 15, 25, 35\}$ and let $\star$ be the operation of multiplication modulo 40. (For example, $15 \star 35 = 5$.) Show that $(G, \star)$ is a group.

   Solution: For this solution, we use "$\cdot$" to denote regular multiplication. First we'll check that $\star$ really is an operation on this set (i.e., that is the product of two of these numbers, mod 40, is always another

one of these numbers). Clearly, the operation is commutative, and so we only need to check the following:

$$\begin{aligned}
5 \cdot 5 = 25, &\quad \text{so } 5 \star 5 = 25 \in G \\
5 \cdot 15 = 75, &\quad \text{so } 5 \star 15 = 35 \in G \\
5 \cdot 25 = 125, &\quad \text{so } 5 \star 25 = 5 \in G \\
5 \cdot 35 = 175, &\quad \text{so } 5 \star 35 = 15 \in G \\
15 \cdot 15 = 225, &\quad \text{so } 15 \star 15 = 25 \in G \\
15 \cdot 25 = 375, &\quad \text{so } 15 \star 25 = 15 \in G \\
15 \cdot 35 = 525, &\quad \text{so } 15 \star 35 = 5 \in G \\
25 \cdot 25 = 625, &\quad \text{so } 25 \star 25 = 25 \in G \\
25 \cdot 35 = 875, &\quad \text{so } 25 \star 35 = 35 \in G \\
35 \cdot 35 = 1225, &\quad \text{so } 35 \star 35 = 25 \in G.
\end{aligned}$$

Next we'll check associativity. One could do this the long way: for all ways of picking $a, b, c \in G$, verify that $(a \star b) \star c = a \star (b \star c)$, but there are rather a lot of combinations to be checked.

Instead, we'll prove more generally that multiplication modulo n, for any n, is associative. (This is a good example of the paradoxical fact that sometimes it's easier to prove a stronger result.)

Lemma: For any n, multiplication modulo n is an associative operation.

Proof of Lemma: Suppose a, b, and c are integers and $\star$ denotes multiplication modulo n. We aim to show that $(a \star b) \star c = a \star (b \star c)$.

Define r by $r = a \star b$. This means that $a \cdot b = nq + r$ for some integer q (and note that $0 \leq r < n$). Now define s by $s = r \star c$, so that $r \cdot c = np + s$. Combining these tells us that

$$(a \cdot b) \cdot c = (nq + r) \cdot c = nqc + rc = nqc + np + s = n(qc + p) + s. \tag{1}$$

Now repeat the same argument, starting from $a \star (b \star c)$ instead of from $(a \star b) \star c)$. Define $\widehat{r}$ by $\widehat{r} = b \star c$ and $\widehat{s}$ by $\widehat{s} = a \star \widehat{r}$, and the same logic as before shows that

$$a \cdot (b \cdot c) = n(\widehat{q}a + \widehat{p}) + \widehat{s}, \tag{2}$$

where $\widehat{q}$ and $\widehat{p}$ are the versions of q and p for this paragraph.

Look at the leftmost parts of Equations (1) and (2). They are $(a \cdot b) \cdot c$ and $a \cdot (b \cdot c)$, which are equal because regular multiplication is associative. Hence,

$$n(qc + p) + s = n(\widehat{q}a + \widehat{p}) + \widehat{s}.$$

As s and $\widehat{s}$ are both between 0 and $n - 1$ (inclusive), it must be true that $s = \widehat{s}$. Since $s = (a \star b) \star c$ and $\widehat{s} = a \star (b \star c)$, we've proved associativity. □

Moving along, we must show that G has an identity. Examining the multiplication table above, we find that $a \star 25 = a$ for all $a \in G$. (We don't need to also check that $25 \star a = a$ because we've already pointed out that $\star$ is commutative.) So, 25 is the identity of the group.

Lastly we need to find an inverse for each element. Again, by examining the multiplication table we notice that $5 \star 5 = 25$, $15 \star 15 = 25$, $25 \star 25 = 25$ and $35 \star 35 = 25$, so that each element is its own inverse.

We've checked all the necessary properties, so we can conclude that G is a group.

---

4. For any two sets A and B, the *symmetric difference* $A \triangle B$ is defined by

$$A \triangle B = (A \setminus B) \cup (B \setminus A).$$

In other words, the symmetric difference is the set of elements that are in A or in B but not in both.

The *powerset* of a set S, denoted $\mathcal{P}(S)$ is the set of all subsets of S, including the empty set and the full set. For example,

$$\mathcal{P}(\{1,2,3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}.$$

Fix a set S. Prove that $(\mathcal{P}(S), \triangle)$ is a group.

Solution:

It is immediately obvious that $\triangle$ is an operation — if A and B are in $\mathcal{P}(S)$ then they are subsets of S, and $A \triangle B$ is another subset of S, which is also in $\mathcal{P}(S)$.

Next, we examine associativity. We must demonstrate that

$$(A \triangle B) \triangle C = A \triangle (B \triangle C).$$

As always, there are many ways to do this. The approach we'll take here it to consider an arbitrary element $x \in S$ and consider all eight possible cases of whether it's in A, B, or C. (There are eight cases because it's either in A or not, in B or not, and in C or not, and $2 \cdot 2 \cdot 2 = 8$.)

Here's the table, and we'll explain one of the rows as an example afterward.

$x \in A$	$x \in B$	$x \in C$	$x \in A \triangle B$	$x \in B \triangle C$	$x \in (A \triangle B) \triangle C$	$x \in A \triangle (B \triangle C)$
×	×	×	×	×	×	×
×	×	✓	×	✓	✓	✓
×	✓	×	✓	✓	✓	✓
×	✓	✓	✓	×	×	×
✓	×	×	✓	×	✓	✓
✓	×	✓	✓	✓	×	×
✓	✓	×	×	✓	×	×
✓	✓	✓	×	×	✓	✓

Let's explain the table by looking at the third row from the stop. Suppose x is an element of S that is in B but not in A or C. Then, as the fourth and fifth column state, x is in both $A \triangle B$ and $B \triangle C$, and as the sixth and seventh column state, x is in both $(A \triangle B) \triangle C)$ and $A \triangle (B \triangle C)$.

The fact that the sixth and seventh column are identical demonstrates that these two sets contain the same elements, and thus are equal. Hence $\triangle$ is associative.

Next, we claim that the empty set is an identity. Indeed,

$$A \triangle \emptyset = \emptyset \triangle A = (A \setminus \emptyset) \cup (\emptyset \setminus A) = A$$

for all $A \in \mathcal{P}(S)$.

Lastly, we claim that A is always its own inverse. To prove this, note that

$$A \triangle A = (A \setminus A) \cup (A \setminus A) = \emptyset.$$

Therefore, $(\mathcal{P}(S), \triangle)$ is a group.