HW 1 - MATH403

Danesh Sivakumar

June 14, 2022

Problem 1 (Chapter 2, Exercise 4)

Which of the following sets are closed under the given operation?

(a) $\{0, 4, 8, 12\}$ addition mod 16

(b) $\{0, 4, 8, 12\}$ addition mod 15

(c) $\{1, 4, 7, 13\}$ multiplication mod 15

(d) $\{1, 4, 5, 7\}$ multiplication mod 9

Proof.

(a) Given the Cayley table:

	0	4	8	12
0	0	4	8	12
4	4	8	12	0
8	8	12	0	4
12	12	0	4	8

We observe that all entries in the table are in the set; thus the group is indeed closed.

(b) Note that $(4 + 12) \bmod 15 = 1 \notin G$; thus the group is not closed.

(c) Given the Cayley table:

	1	4	7	13
1	1	4	7	13
4	4	1	13	7
7	7	13	4	1
13	13	7	1	4

We observe that all entries in the table are in the set; thus the group is indeed closed.

(d) Note that $(4 \cdot 5) \bmod 9 = 2 \notin G$; thus the group is not closed.

$\square$

Problem 2 (Chapter 2, Exercise 16)

Show that the set $\{5, 15, 25, 35\}$ is a group under multiplication modulo 40. What is the identity element of this group? Can you see any relationship between this group and $U(8)$?

Proof. Given the Cayley table of this group:

	5	15	25	35
5	25	35	5	15
15	35	25	15	5
25	5	15	25	35
35	15	5	35	25

We observe that all entries in the table are in the set; thus the group is indeed closed. Furthermore, note that 25 is the identity; that is, it is the element e with the property that for any $a \in G$, $a \cdot e = a$. Now, given the Cayley table of $U(8)$:

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

We observe that each element of the original group corresponds to an element of $U(8)$; namely, 5 corresponds to 5, 15 corresponds to 7, 25 corresponds to 1, and 35 corresponds to 3.

$\square$

Problem 3 (Chapter 2, Exercise 32)

Construct a Cayley table for $U(12)$.

Proof.

	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

$\square$

Problem 4 (Chapter 2, Exercise 36)

Let a and b belong to a group G. Find an x in G such that $xabx^{-1} = ba$.

Proof. Suppose $a, b, x \in G$ with the property that $xabx^{-1} = ba$. Then

$$xabx^{-1} = ba$$
$$xabx^{-1}x = bax$$
$$xabe = bax$$
$$xab = bax$$

Matching terms, we get that $x = b$ works. We know that $b^{-1} \in G$ because $b \in G$, so:

$$babb^{-1} = bae = ba$$

Similarly, $x = a^{-1}$ works:

$$a^{-1}aba = eba = ba$$

$\square$

Problem 5 (Chapter 2, Exercise 46)

Prove that the set of all 3×3 matrices with real entries of the form

$$A = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

is a group.

Proof. Multiplication is defined as follows:

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+a' & b'+ac'+b \\ 0 & 1 & c'+c \\ 0 & 0 & 1 \end{bmatrix}$$

It is clear that $a + a'$, $b' + ac' + b$, and $c' + c$ are each real valued; thus the set is closed under multiplication.

We must first show that the set has an identity element; observe that the identity matrix I_3 is the identity in this group, because:

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

and

$$\begin{bmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix} \cdot \begin{bmatrix}1 & a & b\\0 & 1 & c\\0 & 0 & 1\end{bmatrix} = \begin{bmatrix}1 & a & b\\0 & 1 & c\\0 & 0 & 1\end{bmatrix}$$

Thus $A \cdot e = e \cdot A = A$, with $e = I_3$

Now, we must show that inverses exist. Indeed, by equating coefficients in the definition of multiplication, we get:

$$A^{-1} = \begin{bmatrix}1 & -a & -b+ac\\0 & 1 & -c\\0 & 0 & 1\end{bmatrix}$$

which is in the set, as $-a$, $-b+ac$ and $-c$ are real valued. Multiplying this out yields:

$$\begin{bmatrix}1 & a & b\\0 & 1 & c\\0 & 0 & 1\end{bmatrix} \cdot \begin{bmatrix}1 & -a & -b+ac\\0 & 1 & -c\\0 & 0 & 1\end{bmatrix} = \begin{bmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix}$$

and

$$\begin{bmatrix}1 & -a & -b+ac\\0 & 1 & -c\\0 & 0 & 1\end{bmatrix} \cdot \begin{bmatrix}1 & a & b\\0 & 1 & c\\0 & 0 & 1\end{bmatrix} = \begin{bmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix}$$

Thus $A \cdot A^{-1} = A^{-1} \cdot A = e$

Lastly, we must demonstrate the associative property. Indeed, observe that:

$$\left(\begin{bmatrix}1 & a & b\\0 & 1 & c\\0 & 0 & 1\end{bmatrix} \cdot \begin{bmatrix}1 & d & e\\0 & 1 & f\\0 & 0 & 1\end{bmatrix}\right) \cdot \begin{bmatrix}1 & g & h\\0 & 1 & i\\0 & 0 & 1\end{bmatrix}$$

$$= \begin{bmatrix}1 & a+d & e+af+b\\0 & 1 & c+f\\0 & 0 & 1\end{bmatrix} \cdot \begin{bmatrix}1 & g & h\\0 & 1 & i\\0 & 0 & 1\end{bmatrix}$$

$$= \begin{bmatrix}1 & g+a+d & h+i(a+d)+e+af+b\\0 & 1 & f+c+i\\0 & 0 & 1\end{bmatrix}$$

and

$$\begin{bmatrix}1 & a & b\\0 & 1 & c\\0 & 0 & 1\end{bmatrix} \cdot \left(\begin{bmatrix}1 & d & e\\0 & 1 & f\\0 & 0 & 1\end{bmatrix} \cdot \begin{bmatrix}1 & g & h\\0 & 1 & i\\0 & 0 & 1\end{bmatrix}\right)$$

$$= \begin{bmatrix}1 & a & b\\0 & 1 & c\\0 & 0 & 1\end{bmatrix} \cdot \begin{bmatrix}1 & d+g & h+id+e\\0 & 1 & f+i\\0 & 0 & 1\end{bmatrix}$$

$$= \begin{bmatrix} 1 & g+a+d & h+e+di+a(f+i)+b \\ 0 & 1 & f+c+i \\ 0 & 0 & 1 \end{bmatrix}$$

Thus, given matrices A, B and C, it follows that $(AB)C = A(BC) = ABC$.

All three of the group axioms are satisfied, so this set under multiplication forms a group.

□

Problem 6 (Chapter 2, Exercise 48)

In a finite group, show that the number of nonidentity elements that satisfy the equation $x^5 = e$ is a multiple of 4. If the stipulation that the group be finite is omitted, what can you say about the number of nonidentity elements that satisfy the equation $x^5 = e$?

Proof. Suppose that for $a \in G$, we have $a^5 = e$ with $a \neq e$.
Then, it follows that $(a^2)^5 = (a^5)^2 = e^2 = e$. Suppose FSOC $a^2 = e$, then $(a^2)^2 = a^4 = e^2 = e = a^5$, implying that $a = e$, which is a contradiction, so, $a^2 \neq e$.
Similarly, it follows that $(a^3)^5 = (a^5)^3 = e^3 = e$. Suppose FSOC $a^3 = e$, then $(a^3)^2 = a^6 = e^2 = e = a^5$, implying that $a = e$, which is a contradiction, so, $a^3 \neq e$.
Similarly, it follows that $(a^4)^5 = (a^5)^4 = e^4 = e$. Suppose FSOC $a^4 = e$, then $e = a^4 = a^5$, implying that $a = e$, which is a contradiction, so, $a^4 \neq e$.
We claim that for distinct $i, j \in \{1, 2, 3, 4\}, a^i \neq a^j$. To this end, suppose FSOC that $a^i = a^j$. This is equivalent to $a^{i-j} = e$. WLOG assume $i > j$, then $i - j \in \{1, 2, 3\}$. We previously showed that $a, a^2, a^3 \neq e$, so $a^{i-j} \neq e$, which is a contradiction; thus, $a^i \neq a^j$.
Thus, we deduce that $\{a, a^2, a^3, a^4\}$ are 4 unique nonidentity elements that satisfy $x^5 = e$.
Now suppose that there exists $b \in G$ such that $b^5 = e$, $b \neq e$, and $b \notin \{a, a^2, a^3, a^4\}$. We will show that $\{b, b^2, b^3, b^4\}$ and $\{a, a^2, a^3, a^4\}$ are disjoint.
Suppose FSOC that $b^4 = a^i$ for some $i \in \{1, 2, 3, 4\}$. Then $e = a^i b \implies a^{5-i} = a^{5-i} a^i b \implies a^{5-i} = b$, which is a contradiction, so $b^4 \neq a^i$ for all $i \in \{1, 2, 3, 4\}$
Suppose FSOC that $b^2 = a^i$ for some $i \in \{1, 2, 3, 4\}$. Then $(b^2)^2 = a^{2i} \implies b^4 = a^{2i}$, which contradicts the previous statement, so $b^2 \neq a^i$ for all $i \in \{1, 2, 3, 4\}$
Suppose FSOC that $b^3 = a^i$ for some $i \in \{1, 2, 3, 4\}$. Then $e = a^i b^2 \implies a^{5-i} = b^2$, which contradicts the previous statement, so $b^3 \neq a^i$ for all $i \in \{1, 2, 3, 4\}$
So $\{b, b^2, b^3, b^4\}$ and $\{a, a^2, a^3, a^4\}$ are disjoint, meaning that any $b \notin \{a, a^2, a^3, a^4\}$ will contribute 4 additional distinct solutions; since the group has finitely many elements, the total number of solutions is finite and a multiple of 4, as desired.
If the group is not finite (i.e. is infinite), the group could have infinitely such nonidentity elements that satisfy the equation $x^5 = e$.

□

Problem 7 (Chapter 2, Exercise 52)

Suppose that in the definition of a group G, the condition that for each element a in G there exists an element b in G with the property that $ab = ba = e$ is replaced by the condition that $ab = e$. Show that $ba = e$.

Proof. Let $a \in G$ be arbitrary. By assumption, there exists $b \in G$ such that $ab = e$. Left multiplying this expression by b yields $bab = b$. Right cancellation of b yields $ba = e$, which was to be shown. □

Problem 8 (Chapter 3, Exercise 4)

Prove that in any group, an element and its inverse have the same order.

Proof. Let $a \in G$ be arbitrary with the property that $|a| = n$; that is, that $a^n = e$. Then $e = (aa^{-1})^n = a^n(a^{-1})^n = e(a^{-1})^n = (a^{-1})^n$, so by definition $|a^{-1}| = n$; interchanging the roles of a and a^{-1} proves the reverse implication. □

Problem 9 (Chapter 3, Exercise 14)

Prove that if a is the only element of order 2 in a group, then a lies in the center of the group.

Proof. Suppose that $a \in G$ is the unique element of order 2; that is, that it is the only element such that $a^2 = e$. We deduce that $a = a^{-1}$. We want to show that for all $g \in G$ it follows that $ag = ga$. To this end, let $g \in G$ be arbitrary and consider $b = gag^{-1}$. Squaring both sides yields $b^2 = gag^{-1}gag^{-1} = gaag^{-1} = gaa^{-1}g^{-1} = gg^{-1} = e$. Since a is the only element of order 2, we deduce that $b = a$, so $a = gag^{-1}$; right multiplying both sides by g yields $ag = ga$, which was to be shown. □

Problem 10 (Chapter 3, Exercise 18)

Suppose that a is a group element and $a^6 = e$. What are the possibilities for $|a|$? Provide reasons for your answer.

Proof. Because $a^6 = e$, it follows that $|a| \leq 6$ by definition of order.
Suppose that $|a| = 1$, then $a = e$, meaning $a^6 = e^6 = e$. Thus, $|a| = 1$ is a possibility.
Suppose that $|a| = 2$, then $a^2 = e$, meaning $a^6 = (a^2)^3 = e^3 = e$. Thus, $|a| = 2$ is a possibility.
Suppose that $|a| = 3$, then $a^3 = e$, meaning $a^6 = (a^3)^2 = e^2 = e$. Thus, $|a| = 3$ is a possibility.
Suppose that $|a| = 4$, then $a^4 = e$, meaning $a^6 = e = a^4a^2 = ea^2$, implying that $a^2 = e$, which contradicts the fact that $|a| = 4$. Thus, $|a| = 4$ is not a possibility.

Suppose that $|a| = 5$, then $a^5 = e$, meaning $a^6 = e = a^5 a = ea$, implying that $a = e$, which contradicts the fact that $|a| = 5$. Thus, $|a| = 5$ is not a possibility. Suppose that $|a| = 6$, then $a^6 = e$. Thus, $|a| = 6$ is a possibility.

In summary, the possibilities of $|a|$ are 1, 2, 3, and 6—namely the divisors of 6. $\square$