MTH320 - Abstract Algebra I

HW #1

September 14th, 2020

Question 1:
Let H be the set of all symmetries on an equilateral triangle. Construct the Caley's Table of $(H, \circ)$ and conclude that $(H, \circ)$ is a group.

From class notes, we have the following 6 functions:

$$\left\{ f_1: \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}, f_2: \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}, f_3 = e: \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}, f_4: \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}, f_5: \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}, f_6: \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} \right\}$$

We further know that the binary operator is the composition of the functions. We define the binary operator as per the following example:

$$f_1 \circ f_2 = f_1(f_2)$$

By this, we say for each $a, b, c \in f_n$, we approach it by doing the following. Let us take a for this case and see what happens to a.

1. We first see what a corresponds to in f_2. In this case, it is c
2. Now, we return to f_1 and see what c corresponds to after the rotation, and in this case, it is a

Therefore, if we proceed with the same logic, we go by each of the columns:

$$a \to c \to a$$
$$b \to a \to b$$
$$c \to b \to c$$

So:

$$f_1 \circ f_2: \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} = f_3 = e$$

Now, let us see the case for all 6 functions and their compositions with each other.

$$f_1 \circ f_1: \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} = f_2$$

$$f_1 \circ f_2: \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} = e$$

$$f_1 \circ e: \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} = f_1$$

$$f_1 \circ f_4: \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} = f_6$$

$$f_1 \circ f_5: \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} = f_4$$

$$f_1 \circ f_6: \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix} = f_5$$

We can do the same for all the rows of the Caley table, but they are trivial. So we will no longer work out each individual composition and instead put all the results as per the same standards of the aforementioned technique.

Therefore, we can come up with the following Caley's Table:

$\circ$	f_1	f_2	e	f_4	f_5	f_6
f_1	f_2	e	f_1	f_6	f_4	f_5
f_2	e	f_1	f_2	f_5	f_6	f_4
e	f_1	f_2	e	f_4	f_5	f_6
f_4	f_5	f_6	f_4	e	f_1	f_2
f_5	f_6	f_4	f_5	f_2	e	f_1
f_6	f_4	f_5	f_6	f_1	f_2	e

Table 1.

We have thus constructed the Caley's table for the set of symmetries for an equilateral triangle. Now, what are some things we can conclude from this? We conclude that $(H, \circ)$ is a group because it has closure (all compositions result in elements of the set, H), it has an identity, e, and we will now look for the inverse of each element.

By definition, the inverse of an element is defined as follows: $a \cdot a^{-1} = e$. In this set, all we need to do is look at the Caley table to see what elements composed with each other give us the identity, e.

(i)

$$
\begin{aligned}
f_1^{-1} &= f_2 \quad \text{since } f_1 \circ f_2 = e \\
f_2^{-1} &= f_1 \quad \text{since } f_2 \circ f_1 = e \\
f_3^{-1} &= f_3 \quad \text{since } f_3 = e \text{ and } e \circ e = e \\
f_4^{-1} &= f_4 \quad \text{since } f_4 \circ f_4 = e \\
f_5^{-1} &= f_5 \quad \text{since } f_5 \circ f_5 = e \\
f_6^{-1} &= f_6 \quad \text{since } f_6 \circ f_6 = e
\end{aligned}
$$

Hence, we have found all the inverses, and these inverses are clearly also in the set H. Furhtermore, by observation from the Caley's table, we can see that it is also associative. So, since this is the case, we conclude that $(H, \circ)$ is a group (closure, inverse, identity, associative).

(ii) For all $f \in H$, find $|f|$. Note that $|f|$, or the order of f, is the minimum number of times the binary operation has to be repeated on the f before we obtain the identity, e. We will do one example to show the process and put the final answers for the rest.

To find $|f_1|$, first we do:

$$f_1 \circ f_1 : \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} = f_2$$

Now we do $f_2 \circ f_1$

$$f_2 \circ f_1 : \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} = f_3$$

Since $f_2 \circ f_1 = (f_1 \circ f_1) \circ f_1 = f_3 = e$;
we conclude that $|f_1| = 3$
(Since it took 3 binary operations to get e)

$$
\begin{aligned}
|f_1| &= 3 \quad \text{Since } f_1 \circ f_1 \circ f_1 = e \\
|f_2| &= 3 \quad \text{Since } f_2 \circ f_2 \circ f_2 = e \\
|f_3| &= 1 \quad \text{Since } f_3 = e
\end{aligned}
$$

$$
\begin{aligned}
|f_4| &= 2 \quad \text{Since } f_4 \circ f_4 = e \\
|f_5| &= 2 \quad \text{Since } f_5 \circ f_5 = e \\
|f_6| &= 2 \quad \text{Since } f_6 \circ f_6 = e
\end{aligned}
$$

We have thus found the order of each of the six elements in the group.

(iii) Show that $(H, \circ)$ is a non-Abelian group.

The definition of an Abelian group is that for all Takeelements in a group, the binary operator acting on the elements results in the same outcome, which is another element in the group, regardless of the order the operator is acted.

Mathematically, Let $(D, \cdot)$ be a group. Then: $\forall a, b \in D,\ a \cdot b = b \cdot a \in D$.

To prove that this group is non-Abelian, we need to find just one example where this commutivity does not hold. We can simply refer to the Caley's table to see this.

$$f_1 \circ f_4 = f_6$$

$$f_4 \circ f_1 = f_5$$

Clearly we have shown that $f_4 \circ f_1 \neq f_1 \circ f_4$, and thus the commutative property does not hold for all elements in this group. Therefore, the group is safely concluded to be non-Abelian.

Question 2:

Let C be the set of complex numbers. We know that $(C^*, \times)$ is a group under multiplication. Let n be some fixed positive integer, $n \geqslant 2$, and let H be the set of all the roots of the polynomial $x^n - 1$. i.e.

$$H = \{x \in C^* |\ x^n - 1 = 0\}$$

Prove that $(H, \times)$ is a subgroup of $(C^*, \times)$.

Firstly, we take advantage of the fact that H is a finite subset of C. If we take this into consideration, then we can use a result introduced in the lectures that tells us that if we have a finite subset of a "larger" set, if the larger set is a group, then the subset, under the same binary operator, will also be a group iff it is closed.

In our case, we know that $(C^*, \times)$ is a group, and $H \subset C^*$. Then we need to show that $(H, \times)$ is closed for it to be a subgroup. We proceed as follows:

$$
\begin{aligned}
\text{Let } a, b \in H \quad & a \text{ and } b \text{ are chosen randomly} \\
a \text{ satisfies: } a^n - 1 &= 0 \\
b \text{ satisfies: } b^n - 1 &= 0 \\
a^n = b^n &= 1 \\
\text{We want to show that } a \cdot b &\in H \\
(a \cdot b)^n - 1 &= (a^n) \times (b^n) - 1 \\
&= (1 \times 1) - 1 \\
&= 0
\end{aligned}
$$

$$
\begin{aligned}
\text{Therefore:} \quad (a \times b)^n - 1 &= 0 \\
\text{And thus } a \cdot b &\in H \\
H \text{ is closed.}
\end{aligned}
$$

We have shown that H is closed under the binary operation $\times$. Since it is a finite subset, it is then concluded that $(H, \times)$ is a subgroup of $(C^*, \times)$.

Question 3:

Consider the group $(\mathbb{Z}_{20}, +)$. Find $|1|, |6|, |14|, |15|, |17|, |12|$.

We first find $|1|$ and observe the fact that $k = 1^k$. Then we can proceed and find the rest.

$$\begin{aligned} 1+1+1+\ ....\ +1\,(20\,\text{times}) &= 20 \\ 20 \text{mod} 20 &= 0 \\ \text{Therefore}, |1| &= 20 \end{aligned}$$

Note that by a result introduced in the lectures, if we have some a in a group where the order of a is finite, then $|a^k| = \frac{m}{\gcd(k,m)}$. We also know that for some $k \in \mathbb{Z}_{20}, 1^k = k$ (As per the instructions of the question, but we can also observe this fact very easily).

Using these results, we can go on to find the orders of the remaining five elements.

$$\begin{aligned} |6| = |1^6| &= \frac{|1|}{\gcd(|1|, 6)} \\ &= \frac{20}{\gcd(20, 6)} \\ &= \frac{20}{2} = 10 \\ \text{Therefore}, |6| &= 10 \end{aligned}$$

$$\begin{aligned} |14| = |1^{14}| &= \frac{20}{\gcd(20, 14)} \\ &= \frac{20}{2} = 10 \end{aligned}$$

$$\begin{aligned} |15| = |1^{15}| &= \frac{20}{\gcd(20, 15)} \\ &= \frac{20}{5} = 4 \end{aligned}$$

$$\begin{aligned} |17| = |1^{17}| &= \frac{20}{\gcd(20, 17)} \\ &= \frac{20}{1} = 20 \end{aligned}$$

$$\begin{aligned} |12| = |1^{12}| &= \frac{20}{\gcd(20, 12)} \\ &= \frac{20}{4} = 5 \end{aligned}$$

Question 4:

Let $H = \{2, 4, 6, 8, 10, 12\}$. Let $\cdot$ be the binary operation: multiplication modulo 14. Construct the Caley's table for $(H, \cdot)$

$\cdot_{14}$	2	4	6	8	10	12
2	4	8	12	2	6	10
4	8	2	10	4	12	6
6	12	10	8	6	4	2
8	2	4	6	8	10	12
10	6	12	4	10	2	8
12	10	6	2	12	8	4

Table 2.

Obviously, this is an Abelian group because $\forall a, b \in H,\ a \cdot b = b \cdot a$.

(i) What is e?

for some $d, e \in H$, we have that $d \cdot e = e \cdot d = d$. What element do we have in H such that

$(d \cdot e)(\text{mod}14) = d$?

This element is 8. Notice that, as an example, $(2 \cdot 8)\text{mod}14 = 16\text{mod}14 = 2$. Another example would be $(12 \cdot 8)\text{mod}14 = 96\text{mod}14 = 12$.

$$\text{Obviously}, e = 8$$

(ii) For each $a \in H$, find a^{-1}.

$$\begin{aligned}
2^{-1} &= 4 \quad \text{Since } (2 \cdot)\text{mod}14 = 8 \\
4^{-1} &= 2 \quad \text{Since } (4 \cdot 2)\text{mod}14 = 8 \\
6^{-1} &= 6 \quad \text{Since } (6 \cdot 6)\text{mod}14 = 8 \\
8^{-1} &= 8 \quad \text{Since } (8 \cdot 8)\text{mod}14 = 8 \\
10^{-1} &= 12 \quad \text{Since } (10 \cdot 12)\text{mod}14 = 8 \\
12^{-1} &= 10 \quad \text{Since } (12 \cdot 10)\text{mod}14 = 8
\end{aligned}$$

(iii) Find $|6|$ and $|10|$

$$(6 \cdot 6)\text{mod}14 = 8, \text{therefore } |6| = 2$$

Using a calculator, we can see that

$$1,000,000\text{mod}14 = 8$$

$$10 \cdot 10 \cdot 10 \cdot 10 \cdot 10 \cdot 10 = 1000000$$

$$\text{Therefore}, |10| = 6$$

Question 5:

Part 1:

Let a, b be elements in a group, $(D, \cdot)$ such that $a \cdot b = b \cdot a$. Given that $|a| = n, |b| = m$, where n, $m \neq \infty$ and $\gcd(n, m) = 1$, let $x = a \cdot b$. Prove that $|x| = n\,m$.

Hints:

$$\text{if } a \cdot b = b \cdot a, \text{then } (a \cdot b)^n = a^n \cdot b^n$$

$$\text{if } a \cdot b \neq b \cdot a, \text{we CANNOT conclude } (a \cdot b)^n = a^n \cdot b^n$$

Let k, n, m be positive integers

1. If $n|km$ and $\gcd(n,m)=1$, then $n|k$.
2. If $n|k$ and $m|k$ and $\gcd(n,m)=1$, then we conclude that $nm|k$

In the question, we are given the following facts: $\gcd(n,m)=1$, $|a|=n$, $|b|=m$.

$$\begin{aligned} x &= a\cdot b \\ \text{Let us take } k &= |x| \quad (i.e. x^k = e), k\in\mathbb{Z}^+ \\ \text{Assume } k \text{ to be the smallest positive integer} & \\ \text{such that } x^k &= e \end{aligned}$$

$$\begin{aligned} (a\cdot b)^k &= (a)^k\cdot(b)^k = e \\ \text{We know } a^n &= e \text{ and } b^m = e \end{aligned}$$

By some result introduced in the lectures, we know that if $|a|=n$, and $a^k=e$, then $n|k$. So we can conclude the following:

$$\begin{aligned} n|k, k &\text{ is divisible by } n \\ \frac{k}{n} &= \alpha \quad \alpha\in\mathbb{Z}^+ \\ \text{In other words, } k &= \alpha n \end{aligned}$$

$$\begin{aligned} \text{Furthermore, } m|k & \\ \frac{k}{m} &= \quad \in\mathbb{Z}^+ \\ \text{In other words, } k &= \beta m \end{aligned}$$

By the hint given to us in the question, we know that if $n|k$ and $m|k$, then $nm|k$ (Given that $\gcd(n,m)=1$). In other words, $k=\gamma nm$, for some $\gamma\in\mathbb{Z}^+$.

$$\begin{aligned} (a\cdot b)^{mn} &= a^{mn}\cdot b^{mn} \\ &= (a^n)^m\cdot(b^n)^m \\ a^n &= b^n = e \\ \text{Therefore:} \quad e^m\cdot e^m &= e\cdot e = e \end{aligned}$$

$$\text{Hence } k|mn$$

Since $k|mn$ and $mn|k$, we can logically conclude that $k=mn$. In this case, we can easily see the following:

$$|x| = k = nm$$

$$x^k = x^{mn} = e$$

Part 2:

Find two elements in **Question 1**, f and k in $(H, \circ)$ s.t. $|f| = 2$ and $|k| = 3$, but $|f \circ k| \neq 6$.

Let us take $f = f_4, |f_4| = 2$, and $k = f_1, |f_1| = 3$.

$$f_4 \circ f_1 = f_5$$

$$|f_5| = 2 \neq 6$$

Hence we can clearly see that despite the fact that $\gcd(2,3) = 1$, we cannot claim that $|f_4 \circ f_1| = 6$, in fact we have proven for it to be 2. This is because the group in **Question 1** is NON-Abelian and we cannot say that $a \cdot b = b \cdot a \quad \forall a, b \in H$.