Intro to Proofs: HW10

Aamod Varma

November 14, 2024

Problem 2

Proof. First we see that for (a.) there is no identity element hence it cannot be a group. However for b., c. and d. we have the identity element $e = a$ Now we see that for (d.) there is no inverse element such that it gives us

the identity. The identity is $e = a$ and there is no element d^{-1} such that $d \circ d^{-1} = a$. Hence $(d.)$ is not a group.
So (b) and (c) form a group because we have an inverse element, identity element and is associated as well. ☐

Problem 4

All four side of a rhombus are of equal length, so we can both rotate and reflect and keep it symmetrical. A rhombus has the following symmetries,

1. Identity (I)
2. 180 degree rotation around the center (R)
3. Reflection over vertical axis (V)
4. Reflecting over horizontal axis. (H)

So the table would look like,

	I	R	V	H
I	I	R	V	H
R	R	I	H	V
V	V	H	I	R
H	H	V	R	I

We first see using the table that we have an identity element, an inverse as well as its associative because its similar to the $\mathbb{Z}_4$ Cayley tables.
We also see that the Cayley table for a rectangle is similar to that of a rhombus and is the same as above.

Problem 7

Proof. First we show its a group and then that its abelian.
1. Identity
We have,

$$a * b = a + b + ab$$

So let $a + b + ab = a$ then,

$$\begin{aligned} a + b + ab &= a \\ b + ab &= 0 \\ b(1 + a) &= 0 \end{aligned}$$

So for all a if the rhs has to be zero then $b = 0$. Hence we have,

$$a * b = a \text{ if } b = 0$$

so,

$$a * 0 = a$$

which means we have an identity element.
2. Inverse,
We need b such that $a * b = 0$
So,

$$\begin{aligned} a * b = a + b + ab &= 0 \\ b(1+a) &= -a \\ b &= -\frac{a}{1+a} \end{aligned}$$

Hence we found b such that $a * b = 0$. Which is the existence of inverse $a^{-1} = -\frac{a}{1+a}$
3. Associativity.
We need to show that,

$$(a * b) * c = a * (b * c)$$

First the left hand side evaluates to,

$$(a * b) * c = (a + b + ab) * c = (a + b + ab) + c + c(a + b + ab)$$

$$= a + b + c + ab + ac + bc + abc$$

And the right hand side evaluates to,

$$a * (b + c + bc) = a + b + c + bc + a(b + c + bc)$$

$$= a + b + c + ab + bc + ac + abc$$

So both sides evaluate to the same thing hence it is associative.
Now to show its abelian we need to show that,

$$a * b = b * a$$

So consider $a * b = a + b + ab$ and we have $b * a = b + a + ba$
It is easy to see that this is equal because of associativity and commutativity of the reals. Hence our group is an abelian group. $\square$

Problem 10

Proof. Consider $A = \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix}$
1. Identity

We need to find B such that $AB = A$. So we have,

$$\begin{bmatrix}1 & x & y\\0 & 1 & z\\0 & 0 & 1\end{bmatrix}\begin{bmatrix}1 & x' & y'\\0 & 1 & z'\\0 & 0 & 1\end{bmatrix} = \begin{bmatrix}1 & x & y\\0 & 1 & z\\0 & 0 & 1\end{bmatrix}$$

So by definition we have,

$$\begin{bmatrix}1 & x & y\\0 & 1 & z\\0 & 0 & 1\end{bmatrix} = \begin{bmatrix}1 & x+x' & y+y'+xz'\\0 & 1 & z+z'\\0 & 0 & 1\end{bmatrix}$$

Or that $x+x' = x \Rightarrow x' = 0$, $z+z' = z \Rightarrow z' = 0$ and lastly, $y+y'+xz' = y$ but we have $z' = 0$ hence $y + y' = y \Rightarrow y' = 0$
So we have our identity ,

$$I = \begin{bmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix}$$

2. Inverse
We need to find B such that $AB = I$. So we have,

$$\begin{bmatrix}1 & x & y\\0 & 1 & z\\0 & 0 & 1\end{bmatrix}\begin{bmatrix}1 & x' & y'\\0 & 1 & z'\\0 & 0 & 1\end{bmatrix} = \begin{bmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix}$$

By definition we have,

$$\begin{bmatrix}1 & x+x' & y+y'+xz'\\0 & 1 & z+z'\\0 & 0 & 1\end{bmatrix} = \begin{bmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix}$$

This means that $x + x' = 0 \Rightarrow x' = -x$, $z + z' = 0 \Rightarrow z = -z'$. And we have, $y + y' + xz' = 0, y' = -y - xz' = -y + xz$
So we have,

$$B = \begin{bmatrix}1 & -x & -y+xz\\0 & 1 & -z\\0 & 0 & 1\end{bmatrix}$$

such that $AB = I$ hence B is our inverse A^{-1}
3. Associativity,
we need to show that $(AB)C = A(BC)$
Let

$$B = \begin{bmatrix}1 & x' & y'\\0 & 1 & z'\\0 & 0 & 1\end{bmatrix}$$

and

$$C = \begin{bmatrix}1 & x'' & y''\\0 & 1 & z''\\0 & 0 & 1\end{bmatrix}$$

We have,

$$AB = \begin{bmatrix} 1 & x+x' & y+y'+xz' \\ 0 & 1 & z+z' \\ 0 & 0 & 1 \end{bmatrix}$$

So,

$$(AB)C = \begin{bmatrix} 1 & x+x'+x'' & (y+y'+xz')+y''+(x+x')z'' \\ 0 & 1 & z+z'+z'' \\ 0 & 0 & 1 \end{bmatrix}$$

$$(AB)C = \begin{bmatrix} 1 & x+x'+x'' & y+y'+y''+xz'+xz''+x'z'' \\ 0 & 1 & z+z'+z'' \\ 0 & 0 & 1 \end{bmatrix}$$

Now,

$$BC = \begin{bmatrix} 1 & x'+x'' & y'+y''+x'z'' \\ 0 & 1 & z'+z'' \\ 0 & 0 & 1 \end{bmatrix}$$

So we have,

$$A(BC) = \begin{bmatrix} 1 & x+x'+x'' & y+(y'+y''+x'z'')+x(z'+z'') \\ 0 & 1 & z+z'+z'' \\ 0 & 0 & 1 \end{bmatrix}$$

$$A(BC) = \begin{bmatrix} 1 & x+x'+x'' & y+y'+y''+x'z''+xz'+xz'' \\ 0 & 1 & z+z'+z'' \\ 0 & 0 & 1 \end{bmatrix}$$

It is easy to see that $(AB)C = A(BC)$ □

Problem 14

Proof. 1. Identity
We need, (b, n) such that,

$$(a, m) \circ (b, n) = (a, m)$$

So we have,

$$\begin{aligned} (a, m) \circ (b, n) &= (ab, m+n) \\ (a, m) &= (ab, m+n) \end{aligned}$$

So $ab = a \Rightarrow b = 1$ and $m + n = m \Rightarrow n = 0$
So our identity element is $(b, n) = (1, 0)$
2. Inverse
We need (b, n) such that,

$$(a, m) \circ (b, n) = (1, 0)$$

So we have,

$$
\begin{aligned}
(a, m) \circ (b, n) &= (ab, m + n) \\
(1, 0) &= (ab, m + n)
\end{aligned}
$$

SO $ab = 1 \Rightarrow b = 1/a$ (if a not equal to 0 which is true as $a \in R^*$) and $m + n = 0 \Rightarrow n = -m$
So we have $(b, n) = (1/a, -m)$
3. Associtivity
We need to show that,

$$((a, m) \circ (b, n)) \circ (c, o) = (a, m) \circ ((b, n) \circ (c, o))$$

For the left hand side we have,

$$
\begin{aligned}
((a, m) \circ (b, n)) \circ (c, o) &= (ab, m + n) \circ (c, o) \\
&= (abc, m + n + o)
\end{aligned}
$$

For the right hand side we have,

$$
\begin{aligned}
(a, m) \circ ((b, n)) \circ (c, o) &= (a, m) \circ (bc, n + o) \\
&= (abc, m + n + o)
\end{aligned}
$$

We see that the left side and right side equal to the same thing.
Hence it is associative
Therefore G is a group under this operation. □

Problem 17

Proof. 1. We have the cyclic group $\mathbb{Z}_8$ which are the integer's modulo 8 and on addition. The element are,

$$\{0, 1, 2, 3, 4, 5, 6, 7\}$$

2. We have the symmetries of a square. We have two main operations on a square to preserve symmetry (1). Rotate by 90 degrees (r) and (2). reflection (s) and (3) The identity
So the elements of this group is,

$$\{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$$

□

Problem 25

Proof. We show this by induction.

First we check for the case of $n = 1$. We have,

$$ab^1a^{-1} = (aba^{-1})^1$$
$$aba^{-1} = aba^{-1}$$

Now assume its true for $n = k$ so we have,

$$ab^ka^{-1} = (aba^{-1})^k$$

Now we need to show that $n = k + 1$ holds as well or that,

$$ab^{k+1}a^{-1} = (aba^{-1})^{k+1}$$

Going back to $n = k$ case we have,

$$ab^ka^{-1} = (aba^{-1})^k$$
$$ab^ka^{-1}(aba^{-1}) = (aba^{-1})^k(aba^{-1})$$
$$ab^ka^{-1}aba^{-1} = (aba^{-1})^{k+1}$$
$$ab^kba^{-1} = (aba^{-1})^{k+1}$$
$$ab^{k+1}a^{-1} = (aba^{-1})^{k+1}$$

Which is the $n = k + 1$ case. Hence by induction we show that it is true for all $n \in N$.
Now we consider the case when $n = 0$. Which is,

$$ab^na^{-1} = (aba^{-1})^n$$

$$aa^{-1} = 1$$

and

$$(aba^{-1})^0 = 1$$

So it is true.
Lastly we see that case for $n < 0$. This is equivalent to, doing induction for $n \in N$ for,

$$ab^{-n}a^{-1} = (aba^{-1})^{-n}$$

So first we see the base case which is when $n = 1$ we have,

$$ab^{-1}a^{-1} = (aba^{-1})^{-1}$$

The right hand side becomes,

$$ab^{-1}a^{-1}$$

based on how $^{-1}$ is distributed. Hence it is true for the $n = 1$ case.
Now consider the case for $n = k$. We assume that,

$$ab^{-k}a^{-1} = (aba^{-1})^{-k}$$

We need to show it also holds true for the $n = k + 1$ case that is,

$$ab^{-(k+1)}a^{-1} = (aba^{-1})^{-(k+1)}$$

The $n = k$ case gives us,

$$ab^{-k}a^{-1} = (aba^{-1})^{-k}$$

Now we multiply $(aba^{-1})^{-1}$ on both sides and we get,

$$ab^{-k}a^{-1}(aba^{-1})^{-1} = (aba^{-1})^{-k}(aba^{-1})^{-1}$$

$$ab^{-k}a^{-1}ab^{-1}a^{-1} = (aba^{-1})^{-(k+1)}$$

$$ab^{-k}b^{-1}a^{-1} = (aba^{-1})^{-(k+1)}$$

$$ab^{-(k+1)}a^{-1} = (aba^{-1})^{-(k+1)}$$

□

Which is the $n = k + 1$ case.
Hence we show its true for $n > 0, n = 0$ and $n < 0$

Problem 33

Proof. We need to show that,

$$ab = ba$$

for any elements a, b in our group.
We have,

$$(ab)^2 = a^2b^2$$

$$abab = a^2b^2$$

$$a^{-1}abab = a^{-1}a^2b^2$$

$$bab = ab^2$$

$$babb^{-1} = ab^2b^{-1}$$

$$ba = ab$$

Hence we show its commutative. So its an abelian group. □