Homework 2 **John Waczak**

MTH 343 Date: October 9, 2017

Prof. Ren Guo

3.4.7

*Define $S = \mathbb{R} \setminus \{-1\}$. The operation * is such that $a * b = a + b + ab$. Prove that (S,*) is an Abelian group.*

We must prove 4 things in order for S to be an Abelian group. Members of S must be associate, there must exist an identity element, for each element in S there must exist an inverse element, and (to be Abelian) * must be commutative.

1) let a,b,c $\in$ S then:

$$\begin{aligned}
(a * b) * c &= (a + b + ab) * c \\
&= (a + b + ab) + c + c(a + b + ab) \\
&= a + b + ab + c + ac + bc + abc \\
&= a + b + c + ab + ac + bc + abc \\
a * (b * c) &= a * (b + c + bc) \\
&= a + (b + c + bc) + a(b + c + bc) \\
&= a + b + c + bc + ab + ac + abc \\
&= a + b + c + ab + ac + bc + abc \\
(a * b) * c &= a * (b * c)
\end{aligned}$$

Thus S is associative with *.

2) claim: the identity is $e = 0$

$$\begin{aligned}
a * 0 = a + 0 + a0 = a \\
0 * a = 0 + a + 0a = a
\end{aligned}$$

Thus there is a unique identity e in S

3) for each a in S there exists a unique inverse a^{-1}

$$\begin{aligned}
a + b + ab &= 1 \\
a + b(1 + a) &= 1 \\
b &= \frac{1 - a}{1 + a} \equiv a^{-1} \\
a^{-1} * a &= a + \frac{1 - a}{1 + a} + a\frac{1 - a}{1 + a} \\
&= \frac{a^2 + a + 1 - a + a - a^2}{1 + a} \\
&= \frac{1 + a}{1 + a} \\
&= 1 = a * a^{-1}
\end{aligned}$$

Thus there is a unique inverse for each a in S.

4)

$$\begin{aligned}
a * b &= a + b + ab \\
b * a &= b + a + ba \\
&= a + b + ab \\
\Rightarrow a * b &= b * a
\end{aligned}$$

And thus we have shown that (S,*) is an Abelian group. □

3.4.27

prove that the inverse of $g_1 g_2 ... g_n$ is $g_n^{-1} g_{n-1}^{-1} ... g_1^{-1}$.

We will prove this by mathematical induction. Clearly the base step $n = 1$ is true as g_n are in a group. Now assume that $n = k$ is true we must show that $n = k + 1$ follows.

$$\begin{aligned}
(g_1 g_2 ... g_k g_{k+1})(g_{k+1}^{-1} g_k^{-1} ... g_1^{-1}) &= (g_1 g_2 ... g_k) g_{k+1} g_{k+1}^{-1} (g_k^{-1} ... g_1^{-1}) \\
&= (g_1 g_2 ... g_k) e (g_k^{-1} ... g_1^{-1}) \\
&= (g_1 g_2 ... g_k)(g_k^{-1} ... g_1^{-1}) \\
&= e \\
(g_{k+1}^{-1} g_k^{-1} ... g_1^{-1})(g_1 g_2 ... g_k g_{k+1}) &= g_{k+1}^{-1} (g_k^{-1} ... g_1^{-1})(g_1 g_2 ... g_k) g_{k+1} \\
&= g_{k+1}^{-1} e g_{k+1} \\
&= e
\end{aligned}$$

Thus by mathematical induction, the inverse of $g_1 g_2 ... g_n$ is $g_n^{-1} g_{n-1}^{-1} ... g_1^{-1}$. □

3.4.33

Let G be a group. Suppose $(ab)^2 = b^2 a^2$ for any a,b in G. Prove G is an Abelian group. W.T.S. $ab = ba$

$$\begin{aligned}
(ab)^2 &= a^2 b^2 \\
abab &= aabb \\
a^{-1}abab &= a^{-1}aabb \\
\Rightarrow bab &= abb \\
babb^{-1} &= abbb^{-1} \\
\Rightarrow ba &= ab
\end{aligned}$$

And so we have shown G is commutative and therefore G is Abelian. □

3.4.40

Prove that G is a subgroup of $SL_2(\mathbb{R})$.

We need to show three things:

1. e $\in SL_2(\mathbb{R})$ and e $\in$ G
2. if a,b $\in$ G then ab $\in$ G
3. if a $\in$ G then $a^{-1} \in$ G

1) when $\theta = 0$ we have: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ which is the identity in $SL_2(\mathbb{R})$ as well. We have that:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$
$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

2) let $\gamma, \delta \in \mathbb{R}$, then we have that:

$$\begin{pmatrix} \cos\gamma & -\sin\gamma \\ \sin\gamma & \cos\gamma \end{pmatrix} \begin{pmatrix} \cos\delta & -\sin\delta \\ \sin\delta & \cos\delta \end{pmatrix} =$$
$$= \begin{pmatrix} \cos\gamma\cos\delta - \sin\gamma\sin\delta & -\cos\gamma\sin\delta - \sin\gamma\cos\delta \\ \sin\gamma\cos\delta + \cos\gamma\sin\delta & -\sin\gamma\sin\delta + \cos\gamma\cos\delta \end{pmatrix}$$
$$= \begin{pmatrix} \cos\gamma+\delta & -\sin\gamma+\delta \\ \sin\gamma+\delta & \cos\gamma+\delta \end{pmatrix}$$

And since $\gamma + \delta \in \mathbb{R}$, we have that if a,b are in G, ab is in G.

3) Given a we need to show there exists an inverse in G

$$a = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$
$$det[a] = 1$$
$$\Rightarrow a^{-1} = \begin{pmatrix} -\cos\theta & \sin\theta \\ -\sin\theta & -\cos\theta \end{pmatrix}$$

Thus we have found a^{-1} and we can show that it too is in G by the following:

$$\gamma = \theta + \pi$$
$$a^{-1} = \begin{pmatrix} \cos\gamma & -\sin\gamma \\ \sin\gamma & \cos\gamma \end{pmatrix}$$

Thus since $\gamma \in \mathbb{R}$, we have shown $a^{-1} \in G$. Therefore G is a subgroup of $SL_2(\mathbb{R})$. $\square$

3.4.42

let G be 2x2 group of matrices under addition and $H = \left\{ \begin{pmatrix} a & b \\ c & -a \end{pmatrix} : a, b, c \in \mathbb{R} \right\}$. *Prove H is a subgroup of G.*

1) The identity element is the zero matrix $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ which is in both H and G.

2)

$$\text{let} \quad A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$$
$$B = \begin{pmatrix} a' & b' \\ c' & -a' \end{pmatrix}$$
$$\text{then,} \quad A + B = \begin{pmatrix} a + a' & b + b' \\ c + c' & -a + (-a') \end{pmatrix}$$

Since $-a + (-a) = -(a + a')$ we have that $A + B \in H$ as needed.

3) let $A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$. I claim that $A^{-1} = \begin{pmatrix} -a & -b \\ -c & a \end{pmatrix}$ is the inverse to A.

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

Thus we have shown that H is a subgroup of G. $\square$

4.4.5

find the order of every element in $\mathbb{Z}_{18}$.

Recall that if G is a cyclic group of order n and a in G is a generator we have that if $b = a^k$ then the order of b is $\frac{n}{d}$ where $d = gcd(k, n)$. Thus we can determine the order of each element as follows:

$$\begin{aligned}
|0| &= 1 \\
|1| &= 18 \\
|2| &= 9 \\
|3| &= 6 \\
|4| &= 9 \\
|5| &= 18 \\
|6| &= 3 \\
|7| &= 18 \\
|8| &= 9 \\
|9| &= 2 \\
|10| &= 9 \\
|11| &= 18 \\
|12| &= 3 \\
|13| &= 18 \\
|14| &= 9 \\
|15| &= 6 \\
|16| &= 9 \\
|17| &= 18
\end{aligned}$$