MAT 150A Homework 2

Hardy Jones
999397426
Professor Schilling
Fall 2014

1. We need to show that $a(bc) = (ab)c$

   Proof.

   $$\begin{aligned} a(bc) &= a(b) \\ &= ab \\ &= a \end{aligned} \tag{left}$$

   $$\begin{aligned} (ab)c &= (ab) \\ &= ab \\ &= a \end{aligned} \tag{right}$$

   Since left = right, we have shown that the operation is associative. □

   This law is an identity for sets with exactly one element.

   Proof. Assume that a set with more than one element had this law.

   Choose $a \in S$ with e as the identity.

   Then we want that $ae = a = ea$.

   But we see that $ea = e \neq a$.

   It can be shown that if $e = a$ then the identity law holds. As $ee = e = ee$. □

2. We need to show

   - $\star$ is closed

     Proof. Choose $a, b \in G^O$. $a \star b = ba$ and we know that $ba \in G$, so since the set is the same between G and G^O, we also know $ba \in G^O$.
     Thus, $\star$ is closed. □

   - $\forall a, b, c \in G^O, a \star (b \star c) = (a \star b) \star c$

Proof. Choose $a, b, c \in G^O$.

$$\begin{aligned} a \star (b \star c) &= a \star (cb) \\ &= (cb)a \qquad \text{(left)} \end{aligned}$$

$$\begin{aligned} (a \star b) \star c) &= c(a \star b) \\ &= c(ba) \qquad \text{(right)} \end{aligned}$$

Since we know the underlying group G, we know that it is associative. So left = right since G is associative.
Thus, we have shown that the associativity law holds. □

- $\exists e \in G^O$ s.t. $\forall a \in G^O, a \star e = a = e \star a$

  Proof. Choose $a \in G^O$.
  $a \star e = ea = a$ and $e \star a = ae = a$.
  Thus, we have shown that the identity law holds. □

- $\forall a \in G^O, \exists a^{-1} \in G^O$ s.t. $a \star a^{-1} = e = a^{-1} \star a$

  Proof. Choose $a \in G^O$.
  $a \star a^{-1} = a^{-1}a = e$ and $a^{-1} \star a = aa^{-1} = e$.
  Thus, we have shown that the inverse law holds. □

Since we have shown all four properties of a group, we conclude G^O is a group.

3. Let's name our matrix.

$$A = \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}$$

$$A^2 = AA = \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$$

$$A^3 = A^2A = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$A^4 = A^3A = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}$$

$$A^5 = A^4A = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}$$

$$A^6 = A^5A = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Since we have generated the identity, we have generated all possible elements of this cyclic group.

4. *Proof.*

$$\begin{aligned} ab = aeb = aeeb = aa^7eb = aa^7a^7b \\ &= a^3a^3a^3a^3(a^3b) \\ &= a^3a^3a^3a^3(ba^3) \\ &= a^3a^3a^3(a^3b)a^3 \\ &= a^3a^3a^3(ba^3)a^3 \\ &= a^3a^3(a^3b)a^3a^3 \\ &= a^3a^3(ba^3)a^3a^3 \\ &= a^3(a^3b)a^3a^3a^3 \\ &= a^3(ba^3)a^3a^3a^3 \\ &= (a^3b)a^3a^3a^3a^3 \\ &= (ba^3)a^3a^3a^3a^3 \\ &= baa^7a^7 = baa^7e = baee \\ &= ba \end{aligned}$$

Thus, $ab = ba$ as was to be shown. □

5. (b) We need to show:

- Closure

  Proof. We can actually prove this by enumeration.

  $$1 \times 1 = 1 \in H$$

  $$1 \times -1 = -1 \in H$$

  $$-1 \times 1 = -1 \in H$$

  $$-1 \times -1 = 1 \in H$$

  So every element is in H, thus we have closure. □

- Identity

  Proof. Again, we can prove by enumeration that $e = 1$.

  $$1 \times 1 = 1 = 1 \times 1$$

  $$-1 \times 1 = -1 = 1 \times -1$$

  Thus, the identity exists. □

- Inverse

  Proof. Once again, we prove by enumeration.

  $$1 \times 1 = 1 = 1 \times 1$$

  $$-1 \times -1 = 1 = -1 \times -1$$

  Thus, each element in H has an inverse. □

From these three we have shown that H is a subgroup of G.

(c) H is not a subgroup of G as it lacks an identity element and it lacks inverses.

(d) We need to show:

- Closure

  Proof. Choose $a, b \in H$.
  $a \times b$ is a positive real number. So, we have shown closure. $\square$

- Identity

  Proof. We want $e = 1$ to be the identity. Choose $a \in H$.
  $1 \times a = a = a \times 1$.
  So, we have shown the identity exists. $\square$

- Inverse

  Proof. Choose $a \in H$.
  Since a is a real number there exists $\frac{1}{a} \in H$.
  $a \times \frac{1}{a} = 1 = \frac{1}{a} \times a$.
  So we have shown that inverses exist. $\square$

From these three we have shown that H is a subgroup of G.

(e) H is not a subgroup of G as $H \not\subseteq G$ since every element of H is not invertible.

7. (a) We can enumerate the possibilities with this group.

a^0	a^1	a^2	a^3	a^4	a^5
$a^0a^0 = a^0$	$a^1a^1 = a^2$	$a^2a^2 = a^4$	$a^3a^3 = a^0$	$a^4a^4 = a^2$	$a^5a^5 = a^4$
$a^0a^0 = a^0$	$a^2a^1 = a^3$	$a^4a^2 = a^2$	$a^0a^3 = a^3$	$a^2a^4 = a^4$	$a^4a^5 = a^3$
$a^0a^0 = a^0$	$a^3a^1 = a^4$	$a^2a^2 = a^4$	$a^3a^3 = a^0$	$a^4a^4 = a^2$	$a^3a^5 = a^2$
$a^0a^0 = a^0$	$a^4a^1 = a^5$	$a^4a^2 = a^2$	$a^0a^3 = a^3$	$a^2a^4 = a^4$	$a^2a^5 = a^1$
$a^0a^0 = a^0$	$a^5a^1 = a^0$	$a^2a^2 = a^4$	$a^3a^3 = a^0$	$a^4a^4 = a^2$	$a^1a^5 = a^0$

So, we see two of its elements generate the group. Namely, a^1 and a^5.

(b) We again enumerate the possibilities.
First for order 5.

a^0	a^1	a^2	a^3	a^4
$a^0a^0 = a^0$	$a^1a^1 = a^2$	$a^2a^2 = a^4$	$a^3a^3 = a^1$	$a^4a^4 = a^3$
$a^0a^0 = a^0$	$a^2a^1 = a^3$	$a^4a^2 = a^1$	$a^1a^3 = a^4$	$a^3a^4 = a^2$
$a^0a^0 = a^0$	$a^3a^1 = a^4$	$a^1a^2 = a^3$	$a^4a^3 = a^2$	$a^2a^4 = a^1$
$a^0a^0 = a^0$	$a^4a^1 = a^0$	$a^3a^2 = a^0$	$a^2a^3 = a^0$	$a^1a^4 = a^0$

So, we see 4 of its elements generate the group. Namely, a^1, a^2, a^3, and a^4
And for order 8.

a^0	a^1	a^2	a^3	a^4	a^5	a^6	a^7
$a^0a^0 = a^0$	$a^1a^1 = a^2$	$a^2a^2 = a^4$	$a^3a^3 = a^6$	$a^4a^4 = a^0$	$a^5a^5 = a^2$	$a^6a^6 = a^4$	$a^7a^7 = a^6$
$a^0a^0 = a^0$	$a^2a^1 = a^3$	$a^4a^2 = a^6$	$a^6a^3 = a^1$	$a^0a^4 = a^4$	$a^2a^5 = a^7$	$a^4a^6 = a^2$	$a^6a^7 = a^5$
$a^0a^0 = a^0$	$a^3a^1 = a^4$	$a^6a^2 = a^0$	$a^1a^3 = a^4$	$a^4a^4 = a^0$	$a^7a^5 = a^4$	$a^2a^6 = a^0$	$a^5a^7 = a^4$
$a^0a^0 = a^0$	$a^4a^1 = a^5$	$a^0a^2 = a^2$	$a^4a^3 = a^7$	$a^0a^4 = a^4$	$a^4a^5 = a^1$	$a^0a^6 = a^6$	$a^4a^7 = a^3$
$a^0a^0 = a^0$	$a^5a^1 = a^6$	$a^2a^2 = a^4$	$a^7a^3 = a^2$	$a^4a^4 = a^0$	$a^1a^5 = a^6$	$a^6a^6 = a^4$	$a^3a^7 = a^2$
$a^0a^0 = a^0$	$a^6a^1 = a^7$	$a^4a^2 = a^6$	$a^2a^3 = a^5$	$a^0a^4 = a^4$	$a^6a^5 = a^3$	$a^4a^6 = a^2$	$a^2a^7 = a^1$
$a^0a^0 = a^0$	$a^7a^1 = a^0$	$a^6a^2 = a^0$	$a^5a^3 = a^0$	$a^4a^4 = a^0$	$a^3a^5 = a^0$	$a^2a^6 = a^0$	$a^1a^7 = a^0$

So, we see 4 of its elements generate the group. Namely, a^1, a^3, a^5, and a^7.

(c) If we look at the generators for each of the previous groups, we notice that the elements are generators when $gcd(i, n) = 1$, where i is the element and n is the order of the group. In other words, it is the count of the number of coprimes of n.

But we know that Euler's totient, $\varphi(n)$ provides us with this number.

Euler's totient is defined as:

$$\varphi(n) = n \prod_{p|n}^{n} \left(1 - \frac{1}{p}\right)$$

where p are distinct prime numbers.

We can double check this for the cases above.

- $n = 6$

$$\begin{aligned}\varphi(6) &= 6 \prod_{p|6}^{6} \left(1 - \frac{1}{p}\right) \\ &= 6 \left(\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\right) \\ &= 6 \left(\frac{1}{2}\frac{2}{3}\right) \\ &= 6 \left(\frac{1}{3}\right) \\ &= 2\end{aligned}$$

- $n = 5$

$$\begin{aligned}\varphi(5) &= 5 \prod_{p|5}^{5} \left(1 - \frac{1}{p}\right) \\ &= 5 \left(1 - \frac{1}{5}\right) \\ &= 5 \left(\frac{4}{5}\right) \\ &= 4\end{aligned}$$

- $n = 8$

$$\begin{aligned}
\varphi(8) &= 8\prod_{p|8}^{8}\left(1-\frac{1}{p}\right) \\
&= 8\left(1-\frac{1}{2}\right) \\
&= 8\left(\frac{1}{2}\right) \\
&= 4
\end{aligned}$$

So, in general, we have $\varphi(n)$ generators in a cyclic group.

8. Given some group $(G, \cdot)$ with every element except the identity having order 2. We want to show that $ab = ba$

Proof. Choose $a, b \in G$.

Since every element except the identity has order 2, we have:

$$\begin{aligned}
e &= aa \\
&= aea \\
&= a(bb)a \\
&= (ab)(ba)
\end{aligned}$$

Using this, we have.

$$\begin{aligned}
(ab)(ba) &= e \\
(ab)(ba)(ba) &= e(ba) \\
(ab)e &= e(ba) \\
ab &= e(ba) \\
ab &= ba
\end{aligned}$$

Thus, for every group $(G, \cdot)$ with each element aside from the identity having order 2, the group is abelian. $\square$