1. Summary of basic group facts

In the last problem of Homework 03, you showed that every element of a group must appear exactly once in every row of the multiplication table for that group. A similar proof would show that every element appears exactly once in every column. Let me prove it again here.

**Theorem 1.** Let $G$ be a group, and let $a, b \in G$. The element $a$ appears exactly once in the row of the multiplication table consisting of the products $b \cdot x$, which we’ll call the $b$-row.

**Proof.** The element $a$ occurs in the $b$-row, if the equation

\[ b \cdot x = a \]

has a solution (for $x$, the unknown). Since $G$ is a group, $b$ must have an inverse, which we will call $b^{-1}$. Multiplying both sides of equation (1) by $b^{-1}$ (on the left) gives us

\[ x = b^{-1} \cdot a, \]

which must be a unique element of the group, since $\cdot$ is a binary operation. We see, therefore, that

\[ b \cdot (b^{-1} \cdot a) = a, \]

so $a$ must lie in the $b$-row and the $(b^{-1} \cdot a)$-column. It may be clear to you that the solution to the equation is unique, but we can emphasize this fact with the following. Suppose $x$ and $y$ are both solutions to equation (1). Then

\[ b \cdot x = a \quad \text{and} \quad b \cdot y = a. \]

Therefore,

\[ x = b^{-1} \cdot a \quad \text{and} \quad y = b^{-1} \cdot a, \]

and so $x = y$, since products are unique. This explicitly shows that any two solutions to equation (1) must be equal to each other. \(\square\)

A similar proof shows that every element occurs exactly once in each column. We showed last time that for each element of a group, it’s inverse is unique. It’s even easier to show that the identity is unique.

Suppose $e, e' \in G$ are both identities in the group $G$. Then the following must be true.

\[ e = e \cdot e' = e'. \]

In other words, all identities must be equal to each other. We can summarize in the following theorem.

**Theorem 2.** Let $G$ be a group. $G$ has exactly one identity. For each element $a \in G$, $a$ has exactly one inverse (which we’ll call $a^{-1}$). Every element of $G$ occurs exactly once in each row and column.

This illustrates the fact that, while they have relatively few constraints, groups have a lot of structure. In fact, groups with just one, two, or three elements are completely determined by the properties of a group.

2. 0-, 1-, 2-, and 3-element groups

A group is a set with an associative binary operation defined on it, and furthermore, it has an identity, and every element has an inverse.

1. A set can be empty. Can a group be empty?

2. Consider the following multiplication table. Is it a group?
Table 1. The multiplication table for a group with one element.

<table>
<thead>
<tr>
<th>*</th>
<th>e</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
</tr>
</tbody>
</table>

A group with two elements must have the identity $e$ and another element, which we could call $a$. The identity forces us to fill in the first row and first column as in Table 2.

Table 2. The multiplication table for a group with two elements.

<table>
<thead>
<tr>
<th>*</th>
<th>e</th>
<th>a</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>a</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>a</td>
</tr>
</tbody>
</table>

Since every element of the group must occur in every row and column exactly once, there is only one choice for the remaining cell.

In a group with three elements, we must have $G = \{ e, a, b \}$, and the identity element forces the table to look like Table 3.

Table 3. The multiplication table for a group with three elements.

<table>
<thead>
<tr>
<th>*</th>
<th>e</th>
<th>a</th>
<th>b</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>a</td>
<td>b</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>a</td>
<td>b</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>b</td>
<td>b</td>
</tr>
</tbody>
</table>

3. Is it possible for $a \ast a = e$ in Table 3? If so, fill in the rest of the table.

4. Is it possible for $a \ast a = a$? If so, fill in the rest of the table.

5. Is it possible for $a \ast a = b$? If so, fill in the rest of the table.

3. Generators

All groups must have an identity element $e$. Let’s suppose that we have a group $G$, and it has at least two elements, the identity $e$ and something else $s$. Since $s$ and $s$ are both elements of this group, $s \ast s$ must also be an element of the group. This means that $(s \ast s) \ast s$ must belong to $G$, as well. The binary operation in a group must be associative, so we can just write this as $s \ast s \ast s$ without ambiguity. We will use exponential notation, to save us some writing, and we’ll write

\[
s = s^1 \\
\]
\[
s \ast s = s^2 \\
\]
\[
s \ast s \ast s = s^3 \\
\]
\[
s \ast s \ast s \ast s = s^4 \\
\]

etc.
and these all must be elements of the group \( G \). Furthermore, since \( G \) is a group, the element \( s \) must have an inverse, which we can call \( s^{-1} \). Note that if we multiply \((s^{-1})^3 \ast s^3\), we get

\[
(s^{-1})^3 \ast s^3 = s^{-1} \ast s^{-1} \ast s^{-1} \ast s \ast s \ast s \\
= s^{-1} \ast s^{-1} \ast (s^{-1} \ast s) \ast s \ast s \\
= s^{-1} \ast s^{-1} \ast e \ast s \ast s \\
= s^{-1} \ast s^{-1} \ast s \ast s \\
= s^{-1} \ast (s^{-1} \ast s) \ast s \\
= s^{-1} \ast e \ast s \\
= s^{-1} \ast s \\
= e
\]

(8)

In other words, \((s^{-1})^3\) is the inverse of \( s^3 \). It makes sense, therefore, for us to use the notation

\[
(s^{-1})^3 = s^{-3},
\]

and

\[
s^{-3} \ast s^3 = s^{-3+3} = s^0 = e.
\]

Exponential notation works precisely as we’re used to, even though \( \ast \) may have nothing to do with regular multiplication.

I will use the symbol \( \mathbb{Z} \) for the integers. We have that, if \( s \in G \), then \( s^n \in G \) for any \( n \in \mathbb{Z} \). Now, this is not to say that \( G \) must be infinite. We know that’s not true. It may be, for example, that \( s^3 = s^7 \). If this were the case, then we would also know the following.

\[
s^3 = s^7 \\
\ast s^{-3} \ast s^3 = s^{-3} \ast s^7 \\
e = s^4.
\]

(11)

This can be true, if \( s = e \) or \( s^2 = e \), but if not, the number 4 will be important to us.

**Definition 1.** For a group \( G \), if \( s \in G \) and \( n \) is smallest positive integer such that \( s^n = e \), we will say that \( s \) has order \( n \). Only the identity can have order 1, and if \( s^n \) is never \( e \), then the order of \( s \) is \( \infty \).

We can often describe a group by giving the order of a few elements (which we’ll call *generators*) and saying how these elements interact. For example, consider the smallest group \( G \) that satisfies the following: \( s, t \in G \), \( s \) has order 3, \( t \) has order 2, and \( t \ast s = s^2 \ast t \). These three “rules” allow us to simplify any expression involving \( s \) and \( t \). For example,

\[
s^7 = s^3 \ast s^3 \ast s = e \ast e \ast s = s,
\]

and

\[
t^3 \ast s^7 \ast t^5 = t \ast s \ast t \\
= (t \ast s) \ast t \\
= (s^2 \ast t) \ast t \\
= s^2 \ast t^2 \\
= s^2.
\]

(13)

If you think about it, we should always be able to write any expression involving \( s \) and \( t \) as one of the following

\[
G = \{ e, s, s^2, t, s \ast t, s^2 \ast t \}.
\]

(14)

The smallest group including \( s \) and \( t \) and satisfying \( s^3 = e \), \( t^2 = e \), and \( t \ast s = s^2 \ast t \) must have these elements.
4. Homework 04

Problems 1-6 refer to the group $G$ containing $s$ and $t$ with $s^3 = e$, $t^2 = e$, and $t \ast s = s^2 \ast t$. Write your answers in the form $s, t, s^2, s^2 \ast t$, etc., with the $s$'s first.

1. What is $s \ast (s \ast t)$?

2. What is $t \ast s$?

3. What is $(s \ast t) \ast (s \ast t)$?

4. What is $(s^2 \ast t) \ast s^2$?

5. The group $G$ from Problems 1-4 is actually the same as $D_3$ with $s = 120^\circ$ and $t = \cdot$. Which element of $D_3$ corresponds to $s^2$?

6. Which element of $D_3$ corresponds to $s^2 \ast t$?

Problems 7 and 8 refer to the group $H = \{ e, s, s^2, t, s \ast t, s^2 \ast t \}$ that satisfies $s^3 = e$, $t^2 = e$, and $t \ast s = s \ast t$. Note that this last relation is different from $G$, and this relation also makes $H$ abelian.

7. What is $(s \ast t) \ast s^2$?

8. Do any of the elements of $H$ have order 6?

Problems 9 and 10 refer to a group with four elements. The first row and column must look like Table 4.

Table 4. The multiplication table for a group with four elements.

<table>
<thead>
<tr>
<th></th>
<th>e</th>
<th>a</th>
<th>b</th>
<th>c</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>a</td>
<td>b</td>
<td>c</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>b</td>
<td>b</td>
<td>a</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>c</td>
<td>c</td>
<td>c</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>a</td>
<td>a</td>
<td>e</td>
</tr>
</tbody>
</table>

9. Suppose $a \ast a = e$. What is $b \ast c$? (There are two answers. Give both.)

10. Suppose $a \ast a = b$. What is $b \ast c$?

There are four ways you can complete Table 4, but three of these are actually the same. Of the four tables, one has $a, b,$ and $c$ all having order two. In the other tables only one of $a, b,$ and $c$ has order two (the other two have order four).

Bye.