Jonathan Loss

Group Theory Worksheet

Goals:

- To introduce the student to the basics of group theory.
- To provide a historical framework in which to learn.
- To understand the usefulness of Cayley tables.
- To specifically examine the group of the quaternions.

Target Audience:

This worksheet is aimed at providing an introduction to the basics of group theory. It is best suited for those students, whether in high school or undergraduate studies, who have been exposed to set notation and modular arithmetic. There are brief reviews of these operations, and definitions of all major terms are given; yet prior exposure is helpful.

Introduction:

Group theory is a part of a larger branch of mathematics known as abstract or modern algebra. This branch is concerned with different algebraic structures and how they interact with each other more than it is concerned with what the actual elements are. Some other examples of algebraic structures are rings, fields, integral domains, and vector spaces. Group theory was the first of these algebraic structures to be avidly studied. Its roots go back to the 13^{th} and the 15^{th} centuries when the Moors and Leonardo da Vinci studied symmetry independently of each other. Then, in the early 1700s Joseph Lagrange studied permutations of elements (how many different ways the elements of a set could be arranged), but group theory was firmly established as its own field of study in the mid 1800s. Evariste Galois first used the word *group* in its technical sense in a paper he published in 1830. In order to go deeper into understanding the subject, it would be best to give a formal definition of a group at this point:

<u>Definition</u>: A group G is a nonempty set of elements under a binary operation $*$ for which the following four conditions hold:

1) G is closed under the operation $*$: $(a * b) \in G$ when $a, b \in G$.
2) The operation $*$ is associative: $a * (b * c) = (a * b) * c \quad \forall \quad a, b, c \in G$.
3) G has an identity element e: $a * e = e * a = a \quad \forall \quad a \in G$.
4) Each element of G has an inverse: $a * b = b * a = e$.

A formal axiomatic definition, similar to the one above, was first given in a paper published in 1882 by Heinrich Weber. Until that point, mathematicians had been actively working with the concepts of groups, but no one had formally set down a definition.

Examples of Groups:

It would be beneficial to give a few examples of groups so that the reader may better comprehend the definition given above.

<u>Example 1</u>: The set of integers ($\mathbb{Z}$) under the operation of addition is a group.
This set is closed: pick any two integers a and b, and their sum $a + b$ is also an element of the integers. The set is associative since addition on the integers is associative. The identity element is 0. And for any element a, its inverse is $-a$. Therefore it satisfies all the requirements to be a group.

Before proceeding to Example 2, a short review of congruence classes will be discussed. Remember that $x \equiv y \bmod n$ if and only if $x - y$ is a multiple of n. For example, $12 \equiv 6 \bmod 2$ because $12 - 6 = 6$ and $6 = 3 \cdot 2$. Also, $(5 \cdot 8) \equiv 5 \bmod 7$ because $5 \cdot 8 = 40$ and $40 - 5 = 35 = 5 \cdot 7$. You will need this knowledge to answer the questions in Example 2.

<u>Example 2</u>: The set of elements $\{5, 15, 25, 35\}$ under multiplication mod 40 is a group. The product of any two elements in the set is also a member of the set. Associativity holds since multiplication modulo n is associative.

What is the identity element in this set?

What are the inverses of each of the four elements?

<u>Example 3</u>: The set of integers under subtraction is not a group.

Give an example to illustrate why it does not satisfy property 2 of a group.

Give an example to illustrate why it does not satisfy property 3.

<u>Example 4</u>: The set of integers under multiplication is not a group. *Why not?*

Order of a Group:

Another important definition is that of the order of a group. Knowing the order of a group is very useful when working with more advanced group theory, yet it is a very simple concept to understand.

<u>Definition</u>: The order of a group G, denoted $o(G)$ or $|G|$, is the number of elements that the group contains. If G does not have a finite number of elements, its order is said to be infinite.

<u>Example 1</u>: The set $A = \{5, 15, 25, 35\}$ under multiplication mod 40 has order 4, denoted $o(A) = 4$.

<u>Example 2</u>: The set of integers under addition has infinite order because it does not have a finite number of elements.

Cayley Tables:

One of the integral founders of group theory (and abstract algebra in general) was Arthur Cayley (1821-1895). He performed much-needed research in the field that led to the development of what is known today as Cayley's Theorem. The details of that theorem are beyond the scope of this exercise, but he also contributed in another area of group theory that is useful to us here.

Cayley organized the elements of a group along the top and left hand sides of a table. He then filled in the middle with the result of a certain operation performed on two elements. For example, consider the set of complex numbers $G = \{1, -1, i, -1\}$ under multiplication. Cayley would have described their interaction through a table similar to the one that follows:

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

This Cayley table displays all the possible products when two elements are multiplied together. It is read as an element on the left column times an element on the top row. Notice, in this case it does not matter which way you think of doing the multiplication. The top times the left will equal the left times the top. This is because multiplication in this group is commutative; i.e., $ab = ba \;\; \forall \;\; a,b \in G$. However, this is not true in all groups. (Groups that are commutative are also known as Abelian groups, after the Norwegian mathematician Niels Abel who worked with the theory of equations in the early 1800s.)

Fill in the following Cayley table based on the group $G = \{5,15,25,35\}$ under multiplication modulo 40:

$\times$	5	15	25	35
5				
15				
25				
35				

Is this group Abelian?

The Quaternions:

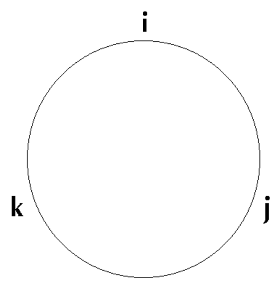
A special group that stands out for its importance to group theory is that of the quaternions, $\{\pm 1, \pm i \pm j, \pm k\}$. William Hamilton discovered this group in 1843 after extensive research. This group is used to extend the complex numbers into three and four dimensions, but its most famous quality is one that we will discover later in this exercise.

An interesting account of how Hamilton discovered the quaternions is found in a letter he wrote to his son many years after the discovery (the excerpt that follows was taken from Gallian, 2002, p. 517):

> But on the 16th day of the same month [October 1843]—which happened to be a Monday and a Council day of the Royal Irish Academy—I was walking to attend and preside, and your mother was walking with me, along the Royal Canal, to which she had perhaps been driven; and although she talked with me now and then, yet an under-current of thought was going on in my mind, which gave at last a result, whereof it is not too much to say that I felt at once the importance. An electric circuit seemed to close; and a spark flashed forth, the herald (as I foresaw immediately) of many long years to come of definitely directed thought and work, by myself if spared, and at all events on the part of others, if I should ever be allowed to live long enough distinctly to communicate the discovery. I pulled out on the spot a pocket-book, which still exists, and made an entry there and then. Nor could I resist

> the impulse—unphilosophical as it may have been—to cut with a knife on a stone of Brougham Bridge, as we passed it, the fundamental formula with the symbols i, j, k;
> $$i^2 = j^2 = k^2 = ijk = -1,$$
> which contains the solution of the Problem, but of course as an inscription, has long since mouldered away.

Hamilton, in his letter above, denoted one of the basic properties of this group: the fact that squaring any of the elements i, j, or k, will produce the number -1. Also, $ij = k = -ji, jk = i = -kj, ki = j = -ik$ **.** It is helpful to think of the multiplication of these elements by using the following circle:



Going in a clockwise manner, multiplying two consecutive elements yields the third element. Going counter-clockwise yields the negative of the third element.

The following Cayley table has been partially filled in. *Use your knowledge of the multiplication in the quaternions in order to fill in the remaining entries.*

□	1	−1	i	$-i$	j	$-j$	k	$-k$
1	1							
−1		1	$-i$					
i			−1		k			
$-i$							j	
j					−1		i	
$-j$			k					
k			j				−1	
$-k$					i			

What is the order of the quaternions?

Is this group Abelian? If not, give an example.

You have just discovered one of the most important properties of this group. It is non-Abelian! This is noteworthy, for it was the first ring (an extension of the idea of a group) to be discovered that was non-commutative.

References:

Two textbooks were extremely useful in the creating of this worksheet. They helped foster ideas for examples and increased my knowledge on the subject itself. They are as follows:

Gallian, J.A. (2002). *Contemporary Abstract Algebra* (5th ed.). New York: Houghton Mifflin.

Gilbert, J. & L. Gilbert. (2000). *Elements of Modern Algebra* (5th ed.). Pacific Grove: Brooks/Cole.