Chapter 2

2.1 The Defining Properties of a Group

A group is a collection of elements that are interrelated according to a set of rules. In mathematics there are 4 rules that all elements must obey to form a group.

1) The product of any 2 elements in a group and the square of each element must also be a member of the group. Note that here, the word "product" does not necessarily mean 'multiply' in the traditional sense of the word (e.g. 2*3 = 6). You can think of the word product as meaning "act on" or "operate on." Where we must agree on what those phrases mean. Thus, addition, subtraction, multiplication, and division could all, in principle, be "products." Most groups you will encounter will obey the commutative law of multiplication, however it is not a requirement that they do so. Groups whose members obey the commutative law are Abelian (i.e. $AB = BA$).
2) One element must commute with all others and leave them unchanged. This is the identity element and is typically represented by "E." Thus, EA = AE = A.
3) The associate law of multiplication must hold. (i.e. $(AB)C = A(BC)$ or $A(BD)(DE) = (AB)(CD)E$)
4) Every element must have a reciprocal that is also a member of the group.

E is always its own reciprocal. Other elements may or may not be their own reciprocals. In general, if A and B are reciprocals, then $AB = BA = E$ and $A^{-1} = B$ and $B^{-1} = A$. Note that only two possibilities for reciprocals exist: (1) an element may be its own reciprocal (e.g. E) or (2) two elements may be reciprocals of each other.

Theorem: The reciprocal of a product equals the product of the reciprocals in reverse order. (i.e.

$$(ABC\ldots)^{-1} = \ldots C^{-1}B^{-1}A^{-1}$$

Proof: Let $AB = C$

$ABB^{-1}A^{-1} = CB^{-1}A^{-1}$

$AEA^{-1} = CB^{-1}A^{-1}$

$AA^{-1} = CB^{-1}A^{-1}$

$E = CB^{-1}A^{-1}$

Thus C must be the reciprocal of $B^{-1}A^{-1}$, but from the first line of the theorem we know that $C = AB$, so $C^{-1} = (AB)^{-1}$. Now $C^{-1}AB = E$ so $C^{-1} = (AB)^{-1} = B^{-1}A^{-1}$ and the theorem is proved.

2.2 Some Examples of Groups

As the book points out a common group would be the integers (…, -2, -1, 0, 1, 2, …) with the function 'addition' chosen as the product, subtraction works just as well, but multiplication and division do not. Do you see why? Consider the 4 rules listed in the previous section:

1) The sum of any two integers yields a third integer. For example, 2 + 3 = 5 and -3 + 2 = -1. Since adding is commutative the group is Abelian.
2) The identity element is 0. (e.g. 2 + 0 = 2)
3) The associative law holds: 1 + 2 + 3 = (1 + 2) + 3 = 1 + (2 + 3) = 6
4) Every element has a reciprocal that is a member of the group. Each number's reciprocal is its negative (e.g. 1 & -1).

Group Multiplication Tables

The number of elements in a group is called its order, h. In the previous example $h = \infty$. A convenient way to display the products of all elements in a finite group is to create a group multiplication table (GMT). A GMT will have h rows and h columns. Since products may not

be commutative, the order is defined as (column element) x (row element).

Theorem: Each row and column in a GMT lists each element once and only once. No two rows or two columns may be identical. The result is that each row/column is a unique scrambling of the elements.

Proof: Consider a group with h elements, $E, A_1, A_2, \ldots, A_h$. In the nth row, the products are (in order) $EA_n, A_1A_n, \ldots, A_nA_n, \ldots, A_hA_n$. Since no two elements are the same, no two products can be the same. E.g. if $A_1A_n = A_2A_n$ that implies that $A_1 = A_2$, which is a contradiction of our initial assumption.

Groups of Orders 1, 2, and 3

$h = 1$ This group is trivial. It has only one element, which must be E.

$h = 2$ One element is E, let the other be A. Then,

G_2	E	A
E	E	A
A	A	E

Thus, A is its own reciprocal.

$h = 3$ The elements for this group are E, A, and B. We begin by constructing the first row and column, both of which are predetermined.

G_3	E	A	B
E	E	A	B
A	A		
B	B		

We now have two ways to fill out the rest of the table.

G_3	E	A	B
E	E	A	B
A	A	B	E
B	B	E	A

or

G_3'	E	A	B
E	E	A	B
A	A	E	B
B	B	A	E

The first table, G_3, is acceptable (note that each row contains one and only element and that they follow the rules outlined earlier). The second however is not because columns 2 and 3 each have a repeated element. If one tries to solve this problem, two rows have repeating elements (try this).

Cyclic Groups

The previous group, G_3, is an example of a cyclic group. A cyclic group is one in which all members result from the products of only one member. In this case, $A = A$, $A \times A = A^2 = B$, and $A \times A \times A = A^3 = E$.

All cyclic groups are Abelian. Do you see why this is reasonable? There will always be a cyclic group for each order, although most orders have additional groups possible. Additional types of groups become possible at $h = 4$. We begin with the cyclic group:

G_4	E	A	B	C
E	E	A	B	C
A	A	B	C	E
B	B	C	E	A
C	C	E	A	B

Note that there is always an *E A B C* progression where on each successive row or column the first element is moved to the rear of the queue.

Since this is a cyclic group each element can be written as a power instead of using different symbols for each element. This makes the cyclic nature of the group obvious.

G_4	E	A	B	C
E	E	θ	θ^2	θ^3
A	θ	θ^2	θ^3	E
B	θ^2	θ^3	E	θ
C	θ^3	E	θ	θ^2

How do we form a second group (i.e. one that is different from the cyclic group)? In the

previous example *B* is its own inverse (*B* x *B* = *E*), while *A* and *C* are inverses of each other. One thing to try is to make each element its own inverse.

G_4	*E*	*A*	*B*	*C*
E	*E*	*A*	*B*	*C*
A	*A*	*E*	*C*	*B*
B	*B*	*C*	*E*	*A*
C	*C*	*B*	*A*	*E*

These are the only two possible groups for this order. Why? Elements that are not their own inverses must come in at least pairs. Since *E* is always its own inverse, this leaves 3 other elements. The two groups just developed cover 2 of 3 possibilities. The third possibility has $A^{-1} = B$, $B^{-1} = C$, and $C^{-1} = A$ (or some analogous variation). This combination can't work. You should take a few minutes to try just to demonstrate it to yourself.

Groups of Order 5 and 6

The book informs you that there is a single group of order 5. From what we've seen so far, you know this must be the cyclic (Abelian) group. There are multiple groups of order 6, including the cyclic group. As an exercise, without having the book open, try to construct one of the other groups. What are the relationships between its members (i.e. what are the inverses)?

2.3 Subgroups

One of the two groups you might have constructed at the end of the last section appears at the top of the next page. If you look at it carefully, you'll see that it contains several smaller groups (called subgroups) within it.

G_6	E	A	B	C	D	F
E	E	A	B	C	D	F
A	A	E	D	F	B	C
B	B	F	E	D	C	A
C	C	D	F	E	A	B
D	D	C	A	B	F	E
F	F	B	C	A	E	D

One of the $h = 2$ subgroups within this group.

Besides (E, A) can you find any other subgroups in this table (there are several, including an $h = 3$ subgroup). The list appears below. One small, but significant point is that all groups contain the trivial, one member subgroup E. Also, all of the subgroups must contain the element E. Do you see why? Here are the possible subgroups: (E, A), (E, B), (E, C), (E, D), and (E, D, F).

For the $h = 6$ group, we can see that all of the subgroups have order 1, 2, 3, and 6 (note the whole group is, of course, a subset of itself). These represent the multiplicative factors that make up the number six. This leads us to LeGrange's theorem which says that the order of any subgroup must be a whole number divisor of the group order.

i.e. Assume a group order, h, then the subgroup order, g, is given by $g = \frac{h}{k}$, where g, h, and k are whole numbers.

The book's proof may be a little confusing and the following discussion may help a bit. Assume a group with A_1, A_2, A_3, …, A_n as its members. The subgroup containing all members has $g = n$, so $\frac{h}{k} = \frac{n}{n} = 1 = k$. Now assume another group with A_1, A_2, A_3, …, A_n and B as its members, where A_1, A_2, A_3, …, A_n represent a subgroup. In this case, A_1, A_2, A_3, …, A_n and B can't all be members of the same subgroup. Why not? Recall that one of the subgroup members must be E. Thus, $BE = EB = B$ and this would violate our initial assumption. There are two possible explanations: (1) the initial assumption is not valid or (2) the products are not members

of the subgroup.

We'll begin by considering the second option. If this is really a group, then BA_1, BA_2, …, BA_n must also be members of the group, so the total number of group members must be 2n (A_1, A_2, …, A_n and BA_1, BA_2, …, BA_n). So h/g = 2n/n = 2 = *k*. What happens if the group consists of the elements A_1, A_2, …, A_n, *B*, and *C*? Now A_1, …, A_n, BA_1, …, BA_n, and CA_1, …, CA_n must be members of the group and if they are mutually exclusive, then *k* = 3. This progression will continue until the product of A_1, …, A_n with other elements yields the total group order, *h*. As you can see from the progression, *k* must always be a whole number.

2.4 Classes

In addition to subgroups, elements may be subdivided into classes. This is accomplished by applying similarity transforms to the elements. Assume *A*, *B*, and *X* are elements in a group where $X^{-1}AX = B$. *B* is called the similarity transform of *A* by *X*. *A* and *B* are said to be conjugate.

Properties of Conjugate Elements

1) Every element is conjugate with itself. That is, there is some element in any group that will convert *A* into itself. *E* will always do this, as well as any element that commutes with *A* ($X^{-1}AX = X^{-1}XA = A$).
2) If *A* is conjugate with *B*, the *B* is conjugate with *A*. Thus, if $X^{-1}AX = B$ then $Y^{-1}BY = A$ where $X = Y^{-1}$.
3) If *A* is conjugate with *B* and *C*, then *B* and *C* are conjugate with each other.

A complete set of elements conjugate to each other is a class. The orders of all classes must be whole number factors of the group.