Introduction to Abstract Algebra: Group Theory

For thousands of years mathematics was exclusively focused on the natural numbers, and extensions of those, plus geometry: in short, it was concerned with mensuration. That began to change, a little, when Euler in 1761 published a study of modular arithmetic. About 1800 Gauss extended Euler's study of congruences and proved, for instance, that a cyclic group of composite order g has subgroups of order d for every natural number d that divides g (although he did not use that terminology). Lagrange studied permutations as part of his investigations into the theory of equations. Both Abel and Galois, who showed that the general quintic equation has no solution in radicals (i.e., an equation of the fifth degree cannot always be solved by addition, multiplication, and root extraction) utilized concepts that were later formalized as *group theory*.

So what does a group look like? Some examples are familiar: for instance, the set of all positive rational numbers (excluding zero) is an infinite group under ordinary multiplication. Similarly, the positive and negative integers form an infinite additive group under addition (no multiplication allowed). Other groups are less familiar. For instance, the process of *permuting* three distinct objects in all possible ways generates a non-commutative finite group of order six.

So what is a group, exactly? A group is a finite or infinite set of elements G and an associated operation $\star$ that satisfy four axioms:

- **Closure:** For all $a, b \in G, a \star b \in G$.
- **Identity:** There exists an identity element I such that $a \star I = I \star a$ for all $a \in G$.
- **Inverses:** For every $a \in G$, there exists a^{-1} such that $a \star a^{-1} = a^{-1} \star a = I$.
- **Associativity:** For all $a, b, c \in G, (a \star b) \star c = a \star (b \star c)$.

In general, the group operation $\star$ does not have to be commutative; the order of operations is important. So in general, $a \star b \neq b \star a$. If the group is commutative we say that the group is a *commutative group*, also called an *Abelian group* in honor of Neils Abel, one of the originators of group theory. Notice that the identity element commutes with every element in any group G, and an element of G always commutes with its inverse. In all other cases, the order of operations is important.

The first groups that mathematicians encountered were based on the natural numbers, so they were commutative groups. Although the axiomatic archetype of a group operation is neither addition nor multiplication, there are a great many examples of groups that do employ everyday arithmetic operations. If the identity element in such a group is 0 and the inverse of a is $-a$, we speak of an *additive group*. Similarly, in a *multiplicative group* the identity element is 1, the operation is ordinary multiplication, and $a^{-1} = 1/a$.

The set of natural numbers $\mathbb{N}$ is not a group under either addition or multiplication because there are no inverse elements in $\mathbb{N}$. The set of all positive and negative integers $\mathbb{Z}$ is an infinite additive Abelian group: $\mathbb{Z}$ is closed under addition, there is an additive identity element 0, every element n has an additive inverse $-n$, and $(l+m)+n = l+(m+n)$ for all $l, m, n \in \mathbb{Z}$. Similarly the set $\mathbb{Q}^+$ of all positive rational numbers m/n is an infinite multiplicative group. as you can easily verify.

How about some finite groups? Well, the simplest possible group is the number 0, under addition (or 1, with multiplication). 0 is the identity element, the group is closed ($0+0=0$), 0 is its own inverse, and $(0+0)+0=0=0+(0+0)$. For obvious reasons, this is called the *trivial group*.

OK, so we can build a group with just one element. How about two elements? Well, $\pm\sqrt{1}$ works under ordinary multiplication: 1 is the identity, the group is closed, 1 is its own inverse, as is -1, and the associative law is known to hold for ordinary multiplication. What about three elements? According to the Fundamental Theorem of Algebra, $\sqrt[3]{1}$ has three distinct values, and $\sqrt[n]{1}$ has n distinct (complex) values. Each one of these sets of the roots of unity forms a group, known as a *cyclic group* (also a *cyclotomic group*). And in fact, since this is abstract algebra, we can simply posit the existence of a symbol r that follows the rules for exponentiation such that $r^n = I$ (I the identity element) and also $r^k \neq I$ when $k < n$ and create the cyclic group of order n without referring to any particular number system besides $\mathbb{N}$ (the number of elements in a finite group G, denoted by $|G|$, is called the *order* of G).

Are there any other finite groups besides cyclic groups? Yes, there are many of them. But that's a topic best left for another day. For now let's just think about *permutation groups* which, according to *Cayley's Theorem*, can be used to construct all possible groups, whether finite or infinite. That theorem is a bit complicated. For now, let's just concentrate on understanding what *permutations* are, and how the *composition* of two permutations gives rise to a group operation $\star$.

In combinatorics. a permutation is simply a rearrangement of a set of objects. So if we are given a set of n objects, any rearrangement of those objects is a permutation of them. If there are two elements in the set, only two permutations are possible: $\{a,b\}$ and $\{b,a\}$. With three objects we get six permutations: $\{a,b,c\}, \{a,c,b\}, \{b,a,c\}, \{b,c,a\}, \{c,a,b\}$, and $\{c,b,a\}$. And in fact, there are $n! = 1 * 2 * 3 * \ldots * n$ possible permutations of n objects. It's easy to write them all down explicitly when there are only a few objects, but it gets harder fast because $n!$ grows pretty quickly.

So how does a rearrangement of objects become a binary operation on the elements of a group? By *composition* of the rearrangements; that is, by performing one rearrangement after another. For this to work, we must understand that each permutation is to be applied to the relative positions of the three objects: "a" always means the first object, "b" always means the second object, and "c" means the third object. So if the permutation (c,b,a) is applied to the set $\{a,b,c\}$ the result is $\{c,b,a\}$; applying (c,b,a) to the set $\{c,b,a\}$ gives the result $\{a,b,c\}$. We conclude that $(c,b,a) \star (c,b,a) = (a,b,c)$.

It should be apparent that with the operation of composition of two permutations understood this way, the group member (a,b,c) is the identity element I. (a,b,c) leaves the order of the elements unchanged, so $(a,b,c) \star (a,b,c) = (a,b,c)$; $(a,b,c) \star (a,c,b) = (a,c,b)$; and so forth. Let's relabel the six permutations as follows: $I = (a,b,c)$, $a = (a,c,b)$, $b = (b,a,c)$, $c = (b,c,a)$, $d = (c,a,b)$, and $e = (c,b,a)$. Using these abbreviations we can construct a sort of multiplication table (also called a Cayley Table after Arthur Cayley, who was the first mathematician to use such tables) for this group as follows.

Cayley Table For S_6, the Symmetric Group of Order Six

	I	**a**	**b**	**c**	**d**	**e**
I	I	a	b	c	d	e
a	a	I	c	b	e	c
b	b	d	I	e	a	d
c	c	e	a	d	I	a
d	d	b	e	I	c	b
e	e	c	d	a	b	I

Unlike the cyclic groups we have examined earlier, S_6 is not a commutative group. We can easily see that the elements I and e commute with every other element. That accounts for twenty of the thirty-six (6×6) possible pairings. There are four additional perfect squares: $(a \star a,\ b \star b,\ c \star c,$ and $d \star d)$. Also, $c \star d = I = d \star c$. So there are 26 pairs of elements that commute under this group operation, and 10 that don't. This permutation group, the symmetric group with six elements, is the smallest possible non-commutative group. All the groups of order 5 or less are cyclic groups (which are always commutative) except for one group of order 4 known as the Klein 4-group: it consists of an identity element plus three elements of order 2. As an exercise, try building the Cayley tables for some of those groups (of order $2, 3, 4, 5$) by yourself.

Additional Concepts: Subgroups and Mappings

If you look at the Cayley table for S_6 closely, you may notice some interesting patterns. For example, $a \star a = b \star b = e \star e = I$; each of these three elements is its own inverse, so the three subsets $\{I, a\}$, $\{I, b\}$, and $\{I, e\}$, when adjoined to the operation $\star$, form three cyclic groups of order 2 that are embedded in S_6. It's a little harder to see, but the three elements $\{I, c, d\}$, plus $\star$, form a cyclic group of order 3, also embedded in S_6. We say that a little group that fits inside a group G is a *subgroup* of G. It should be clear that every group G contains at least two subgroups: the *trivial subgroup* $\{I\}$, and the *improper subgroup* $\{G\}$, itself.

Lagrange's theorem states that the order of a subgroup always divides the order of the group containing it. We won't prove Lagrange's theorem here. But we will define exponentiation in a group by saying that $a^1 = a$, and $a^{n+1} = (a^n) \star a$. Then every element a of a group G has an order n, which we define as the smallest natural number n such that $a^n = I$. Clearly, if the order of G is k, then $a^k = I$ for every a in G. (Do you see why?) So the order of each element a must divide the order of G, by the power law for exponents.

How we can tell if two groups are similar, or the same? In some cases, this is fairly obvious. For instance. it is fairly easy to show that any finite group G of prime order p must have a generating element of order p so that $G = \{r, r^2, r^3, \ldots, r^p = I\}$; every finite group of prime order is a cyclic group, and any element of G, except the identity element, generates that group.

Sometimes the situation can get more complicated. One of the mechanisms algebraists have devised to measure how similar two groups are to one another is called a *holomorphism*. A homomorphism is a function that maps a group G onto another group H and that preserves the group operation. That is to say, a function $f(G)$ is holomorphic if and only if

1. $f : G \to H$ (that is, $f(a) \in H$ for all $a \in G$), and
2. $f(a \star b) = f(a) \star f(b)$ for all $a, b \in G$.

Notice that it is not necessary for a holomorphism to have every $b \in H$ in its range, or codomain. That is, the set of elements in $f(G)$ need not include every $b \in H$. Nor must each $a \in G$ have a unique image in H; we may discover holomorphisms for which $a_1 \neq a_2$, but for which $f(a_1) = f(a_2)$. If a particular holomorphism is one-to-one and it maps G onto H, it is *isomorphic*, or an *isomorphism*. In other words, a function $f(G)$ is isomorphic (or a group G is isomorphic to another group H) if and only if

1. $f : G \to H$ (that is, $f(a) \in H$ for all $a \in G$),
2. every element in H has a unique pre-image in G (the map has an inverse), and
3. $f(a \star b) = f(a) \star f(b)$ for all $a, b \in G$.

Briefly, if G and H are holomorphic they are similar; if they are isomorphic, they are the same.