SUBGROUPS

Below is the multiplication table for D_3.

	e	R	R^2	F	FR	FR^2
e	e	R	R^2	F	FR	FR^2
R	R	R^2	e	FR^2	F	FR
R^2	R^2	e	R	FR	FR^2	F
F	F	FR	FR^2	e	R	R^2
FR	FR	FR^2	F	R^2	e	R
FR^2	FR^2	F	FR	R	R^2	e

Since D_3 is a finite group, if we begin with any element in this group and start multiplying it by itself, then eventually we must complete a cycle that ends when we get back to our starting point. In other words, taking the powers of any element in D_3 generates a cyclic group for us, and this also means that we can have smaller groups that are contained inside larger groups, and when that happens, we say that we have a *subgroup* of the larger group.

	e	R	R^2	F	FR	FR^2
e	e	R	R^2	F	FR	FR^2
R	R	R^2	e	FR^2	F	FR
R^2	R^2	e	R	FR	FR^2	F
F	F	FR	FR^2	e	R	R^2
FR	FR	FR^2	F	R^2	e	R
FR^2	FR^2	F	FR	R	R^2	e

A notation that we use for a subgroup generated by a single element such as R is $\langle R \rangle$. Additionally, the set of elements in $\langle R \rangle$ that we generate by taking powers of R is also referred to as *the orbit of R*. Furthermore, if we have any group G and if H is a subgroup of G, then we write $H \leq G$. We should mention, too, that every group G will have at least two subgroups. Namely, the trivial group represented by the identity element e and the group G, itself. Thus, $\{e\} \leq G$ and $G \leq G$ are true for any group.

Before looking at some concrete examples, let's consider how we might determine if some nonempty subset H of a group G is a subgroup or not. First, recall that a group has to satisfy four properties – closure, associativity, identity, and inverses. We get the associative property for free simply because we know that G is a group, and that leaves closure, existence of an identity element, and existence of inverses. However, let's suppose that H is a nonempty set and that both the closure and inverse properties apply. Then if $h \in H$, it immediately follows that there exists $h^{-1} \in H$, and by closure, $e = hh^{-1} \in H$. Thus, all we really need to know is we've got the closure and inverse properties working for us in order to conclude that $H \leq G$, and this leads to the following theorem.

Theorem: Let G be a group and let H be a nonempty subset of G. If for every $h \in H$ we have that $h^{-1} \in H$ (inverses) and if for every $h_1, h_2 \in H$ we have that $h_1 h_2 \in H$ (closure), then it follows that H is a subgroup of G, $H \leq G$.

Actually, if we are dealing with finite groups, then all we really need for a nonempty subset H is the closure property. For example, suppose the closure property applies to H, let $h \in H$ and consider $\langle h \rangle$, the cyclic subgroup generated by h. Since H is closed under the group operation, every element of this cyclic subgroup must be contained in H, and, hence, $h^{-1} \in H$. Thus, for finite groups we can make our theorem even simpler.

Theorem: Let G be a finite group and let H be a nonempty subset of G. If for every $h_1, h_2 \in H$ we have that $h_1 h_2 \in H$ (closure), then it follows that H is a subgroup of G, $H \leq G$.

Now let's go back and look at all the subgroups of D_3. It turns out that there are six subgroups, and while I'll specify them using traditional set notation, I'm going to write the elements in a column instead of a row. This will make our next few topics a little easier to explain. Anyway, you can use the multiplication table above to help you verify that each of these is a subgroup.

$$\{e\}, \begin{Bmatrix} e \\ F \end{Bmatrix}, \begin{Bmatrix} e \\ FR \end{Bmatrix}, \begin{Bmatrix} e \\ FR^2 \end{Bmatrix}, \begin{Bmatrix} e \\ R \\ R^2 \end{Bmatrix}, \begin{Bmatrix} e \\ R \\ R^2 \\ F \\ FR \\ FR^2 \end{Bmatrix}$$

We have one subgroup of order 1, three subgroups of order 2, one subgroup of order 3, and one subgroup of order 6. Notice, too, that all of the orders of the subgroups are divisors of the order of D_3. This is no accident as we will soon see. But first, let's define what we mean by a *coset*.

$$\{e\}, \begin{Bmatrix} e \\ F \end{Bmatrix}, \begin{Bmatrix} e \\ FR \end{Bmatrix}, \begin{Bmatrix} e \\ FR^2 \end{Bmatrix}, \begin{Bmatrix} e \\ R \\ R^2 \end{Bmatrix}, \begin{Bmatrix} e \\ R \\ R^2 \\ F \\ FR \\ FR^2 \end{Bmatrix}$$

If G is a group, H is a subgroup of G, and $a \in G$, then the set we create by multiplying each element of H on the left by a is called a *left coset*, and we denote it by aH. Similarly, if we multiply each element of H on the right by a, then we call that a *right coset* and write Ha. Now before going any further, I want to demonstrate one result. Namely, that if G is a group, H is a subgroup of G, $a \in G$, and $a \notin H$, then $H \cap aH = \varnothing$. To see this, suppose there exists some $h \in H$ such that $ah \in H$. It would then follow by closure that $a = (ah)h^{-1} \in H$, and this violates our assumption that $a \notin H$. Hence, if $a \notin H$, then H and aH contain totally different elements of G. Also, even though we won't give a formal proof of it, it's not difficult to show that H and aH will have the same number of elements, and everything I've said in this paragraph also holds true for right cosets.

Now let's look at the left cosets in D_3 that correspond to the subgroup $H = \left\{ \begin{matrix} e \\ R \\ R^2 \end{matrix} \right\}$. We basically are going to have two left cosets which we can denote as follows.

$$eH = H = \left\{ \begin{matrix} e \\ R \\ R^2 \end{matrix} \right\}, FH = \left\{ \begin{matrix} F \\ FR \\ FR^2 \end{matrix} \right\}$$

Notice a few things now. First, all of our cosets have the same number of elements, and second, since our group *G* has a finite number of elements, we can't keep creating cossets forever! Eventually, there will be no more elements left to put into cosets, and this means most importantly, that the number of elements in the group will be equal to the product of the number of elements in our original subgroup times the number of distinct cosets we have found! This is a very, very important result that was first discovered by Joseph Lagrange (1736 – 1813), and it is known as Lagrange's Theorem.

$$eH = H = \left\{ \begin{matrix} e \\ R \\ R^2 \end{matrix} \right\}, FH = \left\{ \begin{matrix} F \\ FR \\ FR^2 \end{matrix} \right\}$$

Lagrange's Theorem: If G is a finite group and if H is a subgroup of G, then the order of H divides the order of G. In this case, we also call $|G|/|H| = [G:H]$ the index of H in G.

This theorem is so important because it puts some very specific restrictions on what kinds of subgroups are possible. For example, a subset of four elements of D_3 could never be a subgroup of D_3 since $|D_3| = 6$ and four doesn't divide evenly into six. Similarly, for any cyclic group of prime order, the only subgroups we can have are the identity and the whole group itself, since a prime number can only be divided by itself and 1.

Now let's look at the left cosets of D_3 that correspond to subgroups of order 2 Since we have three subgroups of order 2, the three corresponding sets of left cosets are:

$$H = \begin{Bmatrix} e \\ F \end{Bmatrix}, RH = \begin{Bmatrix} R \\ FR^2 \end{Bmatrix}, R^2H = \begin{Bmatrix} R^2 \\ FR \end{Bmatrix}$$

$$H = \begin{Bmatrix} e \\ FR \end{Bmatrix}, RH = \begin{Bmatrix} R \\ F \end{Bmatrix}, R^2H = \begin{Bmatrix} R^2 \\ FR^2 \end{Bmatrix}$$

$$H = \begin{Bmatrix} e \\ FR^2 \end{Bmatrix}, RH = \begin{Bmatrix} R \\ FR \end{Bmatrix}, R^2H = \begin{Bmatrix} R^2 \\ F \end{Bmatrix}$$

Again, we have verified Lagrange's Theorem. Each subgroup *H* above has only 2 elements, and thus, each of its left cosets can only have 2 elements, and we can keep constructing left cosets until we finally run out of elements in the group, and when that happens we see that the number of elements in our group is equal to the number of elements in *H* times the number of left cosets we can form using *H*. Thus, the number of elements in *H* is a divisor of the total number of elements in our group.

$$H = \begin{Bmatrix} e \\ F \end{Bmatrix}, RH = \begin{Bmatrix} R \\ FR^2 \end{Bmatrix}, R^2H = \begin{Bmatrix} R^2 \\ FR \end{Bmatrix} \qquad H = \begin{Bmatrix} e \\ FR \end{Bmatrix}, RH = \begin{Bmatrix} R \\ F \end{Bmatrix}, R^2H = \begin{Bmatrix} R^2 \\ FR^2 \end{Bmatrix}$$

$$H = \begin{Bmatrix} e \\ FR^2 \end{Bmatrix}, RH = \begin{Bmatrix} R \\ FR \end{Bmatrix}, R^2H = \begin{Bmatrix} R^2 \\ F \end{Bmatrix}$$

Now let's continue with D_3 and go back to the subgroup $H = \left\{ \begin{matrix} e \\ R \\ R^2 \end{matrix} \right\}$. As above, we saw that there are 2 left cosets of H in D_3. Namely,

$$H = \left\{ \begin{matrix} e \\ R \\ R^2 \end{matrix} \right\}, FH = \left\{ \begin{matrix} F \\ FR \\ FR^2 \end{matrix} \right\}$$

Similarly, there are going to be only 2 right cosets of H in D_3. In particular,

$$H = \left\{ \begin{matrix} e \\ R \\ R^2 \end{matrix} \right\}, HF = \left\{ \begin{matrix} F \\ FR^2 \\ FR \end{matrix} \right\}$$

Notice from the above that the left coset FH is the same set of elements as the right coset HF, or in other words, $FH = HF$. Do you think this will always happen? Well, the answer is no, but when it does happen, it makes our subgroup very special, and this leads to the following definition.

$$FH = \left\{ \begin{array}{c} F \\ FR \\ FR^2 \end{array} \right\} \qquad HF = \left\{ \begin{array}{c} F \\ FR^2 \\ FR \end{array} \right\}$$

Definition: If G is a group and H is a subgroup of G and if for every $a \in G$ we have that $aH = Ha$ (alternatively, $aHa^{-1} = H$), then we'll call H a *normal subgroup* of G and we'll denote this by $H \triangleleft G$.

Normal subgroups are important because if $H \triangleleft G$, then the left (or right) cosets of *H* in *G* will form a group. For example, if $\mathbb{Z}$ is the group of integers under addition, then the set of even integers is a normal subgroup of $\mathbb{Z}$. This subgroup divides $\mathbb{Z}$ into two cosets which we can designate as *even* and *odd*. Furthermore, if we add even and odd numbers together in the usual way, then we get a group that is *isomorphic* (identical in structure) to $\mathbb{Z}_2$, the cyclic group of order two. We can see this quite clearly by comparing the multiplication tables for the two groups below.

	Even	Odd
Even	Even	Odd
Odd	Odd	Even

	0	1
0	0	1
1	1	0

We'll explore normal subgroups more later on, but for now let $H = \begin{Bmatrix} e \\ F \end{Bmatrix}$ and let's verify that this is not a normal subgroup of D_3. It will suffice to look at the cosets *RH* and *HR*.

$$RH = \begin{Bmatrix} R \\ FR^2 \end{Bmatrix} \neq \begin{Bmatrix} R \\ FR \end{Bmatrix} = HR$$

Thus, not all subgroups are normal subgroups.

At this point we know that the order of a subgroup divides the order of the group, but is the converse true? For example, if we know that $|G| = 24$, does that mean that subgroups of order 2, 3, 4, 6, 8, and 12 will all exist? We'll we can't say that much, but we can say quite a bit thanks to a series of theorems by Norwegian mathematician Ludwig Sylow (1872). He produced a very important collection of theorems for group theory, and the one we'll present now we'll just call the first Sylow theorem.

The First Sylow Theorem: If G is a finite group and if p^n is the highest power of a prime number p that divides the order of G, then G has at least one subgroup of order p^n. This subgroup is called a *Sylow p-subgroup*.

For example, if $|G| = 24 = 2^3 \cdot 3$, then Sylow's Theorem guarantees us that a subgroup of order $2^3 = 8$ exists, and a subgroup of order 3 exists. That's good to know! Also, in our group D_3 above we saw that we have exactly one Sylow 3-subgroup, and we have three Sylow 2-subgroups. Other theorems in group theory extend this result to let us know that if p is any prime and if p^n divides the order of a group G, then G will have a subgroup of order p^n. Thus, if $|G| = 24 = 2^3 \cdot 3$, then G will definitely have some subgroups with orders 2, 2^2, 2^3, and 3.

Now let's recall that D_3 is isomorphic to S_3, and let's look at the multiplication table for

S_3

	$(1)(2)(3)$	$(1\ 2)$	$(1\ 3)$	$(2\ 3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$
$(1)(2)(3)$	$(1)(2)(3)$	$(1\ 2)$	$(1\ 3)$	$(2\ 3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$
$(1\ 2)$	$(1\ 2)$	$(1)(2)(3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$	$(1\ 3)$	$(2\ 3)$
$(1\ 3)$	$(1\ 3)$	$(1\ 3\ 2)$	$(1)(2)(3)$	$(1\ 2\ 3)$	$(2\ 3)$	$(1\ 2)$
$(2\ 3)$	$(2\ 3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$	$(1)(2)(3)$	$(1\ 2)$	$(1\ 3)$
$(1\ 2\ 3)$	$(1\ 2\ 3)$	$(2\ 3)$	$(1\ 2)$	$(1\ 3)$	$(1\ 3\ 2)$	$(1)(2)(3)$
$(1\ 3\ 2)$	$(1\ 3\ 2)$	$(1\ 3)$	$(2\ 3)$	$(1\ 2)$	$(1)(2)(3)$	$(1\ 2\ 3)$

One thing that is very nice about this table is that everything is written in cycle notation. Also, the number of elements in a cycle is what we'll define as the *length* of that cycle, and the length of a cycle is always going to be the order of the cyclic group generated by that cycle. Additionally, if you raise a cycle to the power that is equal to its length, then the result will be the identity. In other words, $(1\ \ 2)^2 = (1)(2)(3)$ and

$(1\ \ 2\ \ 3)^3 = (1)(2)(3)$.

	$(1)(2)(3)$	$(1\ \ 2)$	$(1\ \ 3)$	$(2\ \ 3)$	$(1\ \ 2\ \ 3)$	$(1\ \ 3\ \ 2)$
$(1)(2)(3)$	$(1)(2)(3)$	$(1\ \ 2)$	$(1\ \ 3)$	$(2\ \ 3)$	$(1\ \ 2\ \ 3)$	$(1\ \ 3\ \ 2)$
$(1\ \ 2)$	$(1\ \ 2)$	$(1)(2)(3)$	$(1\ \ 2\ \ 3)$	$(1\ \ 3\ \ 2)$	$(1\ \ 3)$	$(2\ \ 3)$
$(1\ \ 3)$	$(1\ \ 3)$	$(1\ \ 3\ \ 2)$	$(1)(2)(3)$	$(1\ \ 2\ \ 3)$	$(2\ \ 3)$	$(1\ \ 2)$
$(2\ \ 3)$	$(2\ \ 3)$	$(1\ \ 2\ \ 3)$	$(1\ \ 3\ \ 2)$	$(1)(2)(3)$	$(1\ \ 2)$	$(1\ \ 3)$
$(1\ \ 2\ \ 3)$	$(1\ \ 2\ \ 3)$	$(2\ \ 3)$	$(1\ \ 2)$	$(1\ \ 3)$	$(1\ \ 3\ \ 2)$	$(1)(2)(3)$
$(1\ \ 3\ \ 2)$	$(1\ \ 3\ \ 2)$	$(1\ \ 3)$	$(2\ \ 3)$	$(1\ \ 2)$	$(1)(2)(3)$	$(1\ \ 2\ \ 3)$

This is very good to know because this means that if in some permutation group we have an element that is a product of disjoint cycles looking like $(a \quad b)(c \quad d \quad e)$, then we also have by direct multiplication of cycles that $\left[(a \quad b)(c \quad d \quad e)\right]^3 = (a \quad b)^3 (c \quad d \quad e)^3 = (a \quad b)^3 = (a \quad b)^2 (a \quad b) = (a \quad b)$. Something like this can be very helpful in finding useful moves on Rubik's cube because, in this case we see that if we perform the above permutation three times, then the end result is a mere transposition of just two elements.

Now let's go back and think about cosets again. In particular, recall that a subgroup H is normal if for any $a \in G$ we have that $aH = Ha$. Another way to write this latter condition is as $aHa^{-1} = H$. And now let's think again about S_n, the group of all permutations we can make of n objects. This group has order $n!$, and recall that we can classify every permutation as either even or odd depending upon whether we can write it as an even number of transpositions or an odd number of transpositions.

Thus, let's consider two subsets of S_n, $O =$ the set of all odd permutations and $E =$ the set of all even permutations. The set O is clearly not a subgroup because closure is not satisfied. In other words, the product of an odd permutation with an odd permutation is even. O the other hand, E is a subgroup because closure will be satisfied, the product of an even permutation with an even permutation is still even.

Furthermore, I claim that E is a normal subgroup of S_n. To see this, let $a \in S_n$. The a is either an even permutation or an odd permutation. Also, if we write a as a product of transpositions, then notice that a^{-1} can be written as a product of the same number of transpositions but in the opposite order. This is because if a product of transpositions is like flipping on a bunch of switches, then you undo that by flipping them off in the opposite order. Thus, if a is an even permutation, then so is a^{-1}, and if a is odd, then a^{-1} is also an odd permutation. Consequently, if a is an even permutation, then $aEa^{-1} = E$ since we are just multiplying E on both sides by an even permutation. And similarly, if a is an odd permutation, then again $aEa^{-1} = E$ since every product we may form will have the structure (odd)(even)(odd) = even. Thus, E is a normal subgroup of S_n.

We usually give the normal subgroup of even permutations in S_n the name *the alternating group*, and we denote it by A_n. We always have that $A_n \triangleleft S_n$, and since half the permutations in S_n are even, it's always true that $|S_n| / |A_n| = 2$.

At this point, we've learned a lot about subgroups and cyclic groups and what kinds of subgroups can exist in a given group. Also, one of the very important lessons to derive from this discussion is that every group is really generated by cyclic groups that are simply combined in various ways. Thus, let me show you one way in particular to generate a larger group from smaller groups. In particular, let's take the cyclic groups $\mathbb{Z}_2$ and $\mathbb{Z}_3$, and we're going to form what we call the direct product of $\mathbb{Z}_2$ and $\mathbb{Z}_3$ which we'll denote by $\mathbb{Z}_2 \times \mathbb{Z}_3$. To do this, we'll think of forming ordered pairs where the first coordinate is an element of $\mathbb{Z}_2$ and the second coordinate is an element of $\mathbb{Z}_3$.

If we do this, then we'll get a group with $2 \cdot 3 = 6$ elements, and we can write the elements of the group as the set of ordered pairs $\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0,0),(1,0),(0,1),(0,2),(1,1),(1,2)\}$. In this group, for example, we'll have $(1,1) + (1,1) = (0,2)$.

Now there are a few things we should mention. First, what I did here with two groups, we can do with as many groups as we like. For example, if I take the direct product of three groups, then the each element in the resulting group could be expressed as an ordered triple. Second, I don't have to use cyclic groups like I did in this example. I could take the direct product of any number of groups whether they are cyclic or not. And lastly, because I did use cyclic groups in my example, both the group I constructed and the groups I used in the direct product are abelian. When this is the case, we sometimes call the construction a *direct sum* instead of a *direct product,* and we write $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ instead of $\mathbb{Z}_2 \times \mathbb{Z}_3$.

And now, we're ready for a truly amazing result known as *The Fundamental Theorem of Finite Abelian Groups*. As I've mentioned, every group is really constructed by combining cyclic groups in various ways, and when it comes to finite abelian groups, the structure is very simple indeed. In particular, every finite abelian group can be thought of as simply a direct sum of cyclic groups whose orders are always a prime raised to some power. This essentially tells us how to construct every possible finite abelian group, and so now let's end with a statement of this very important theorem. (without proof!)

The Fundamental Theorem of Finite Abelian Groups: Every finite abelian group is isomorphic to a direct sum of cyclic groups, each with order equal to some prime number raised to a power. Furthermore, this decomposition into a direct sum of cyclic groups of prime power order is unique except for the order in which we write down the terms of the direct sum.

As a few examples of this theorem, notice that $\mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$, $\mathbb{Z}_{10} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_5$, and $\mathbb{Z}_{12} \cong \mathbb{Z}_4 \oplus \mathbb{Z}_3$.