DOC BENTON’S FANTASTIC GUIDE TO GROUP THEORY, RUBIK’S CUBE, PERMUTATIONS, SYMMETRY, AND ALL THAT IS!

CHRISTOPHER P. BENTON, PHD
CONTENTS

1. Introduction to Rubik’s Cube
2. Practice – Introduction to Rubik’s Cube
3. Permutations
4. Practice – Permutations
5. Practice – Permutations (Answers)
6. Counting the Number of Permutations in Rubik’s Cube
7. What is a Group?
8. Practice – What is a Group?
9. Practice – What is a Group? (Answers)
10. Some Special Classes of Groups
11. Practice – Some Special Classes of Groups
12. Practice – Some Special Classes of Groups (Answers)
13. Subgroups – Groups Within Groups
14. Practice – Subgroups
15. Practice – Subgroups (Answers)
16. Rubik’s Cube Subgroups
17. Conjugates and Commutators
18. Practice – Conjugates and Commutators
19. Practice – Conjugates and Commutators (Answers)
20. Conjugates and Commutators in Rubik’s Cube
21. Visual Group Theory
22. Practice – Visual Group Theory

23. Practice – Visual Group Theory (Answers)

24. Groups of Small Order

25. Normal Subgroups and Homomorphisms

26. Practice – Normal Subgroups and Homomorphisms

27. Practice – Normal Subgroups and Homomorphisms (Answers)

28. Patterns on Rubik’s Cube

29. Life Lessons from Group Theory and Rubik’s Cube

30. Symmetry is Everywhere!
INTRODUCTION TO RUBIK’S CUBE

Rubik’s cube is a fascinating puzzle that was invented in 1974 by a Hungarian sculptor and professor of architecture named Ernös Rubik, but it wasn’t until 1980 that the puzzle began to be marketed in the United States by Ideal Toy Corporation and, subsequently, became widely popular. The puzzle itself is deceptively simple in appearance. You have a cube with six faces, and each face of the cube is divided into several smaller cubes, and then the faces themselves can be rotated in several directions in order to create an almost unfathomable number of permutations of the colored squares on each little cube. Many a person has spent many an hour trying to figure out how to unscramble their cube only to simply take it apart with a screwdriver and then reassemble it!

When we look at the cube, we quickly realize that there are six basic moves that we can perform on the cube, and we’ll denote these moves by the letters $R$, $L$, $U$, $D$, $F$, and $B$. These moves represent making quarter-turns in the clockwise direction, respectively, of the right face, left face, up face, down face, front face, and back space of the cube. Some
people, however, like to write these letters in the order *BFUDLR* so that it will appropriately be pronounced “befuddler.” If we now want to rotate, for example, the right face of the cube two quarter-turns clockwise, then that move is usually denoted either by $R^2$ or $2R$ or $R_2$. Similarly, we’ll use $R^3$ or $3R$ or $R_3$ to indicate that one should turn the right face of the cube clockwise through three quarter-turns. Notice also that $R^4$ (or $4R$ or $R_4$) is the same as doing nothing at all. Furthermore, if we want to turn the right face a quarter-turn in the counterclockwise direction, then the usual notations for that are either $R^{-1}$ or $R'$ or $r$. Also, when we are specifying a sequence of moves to be performed on the cube, the custom is to specify those moves in order from left to right. Thus, $R^{-1}DR$ means rotate the right face a quarter-turn counterclockwise, then rotate the down face a quarter-turn clockwise, and finally, rotate the right face a quarter-turn clockwise. Also, clockwise and counterclockwise are defined with respect to what we would see if we were looking at a particular face straight on.

As you might imagine, the mathematics of permutations has an awful lot to do with helping us understand the structure of Rubik’s cube, and as you might also guess, the mathematics of symmetry is additionally going to be important. Fortunately, there is one branch of higher mathematics that covers both of these things, and it is known as *group theory*. Thus, this book is going to be both a brief introduction to the wonders of group theory and to the wonders of Rubik’s cube, and how the knowledge of one can help us with the other. Your first task, though, is simply to buy a Rubik’s cube and learn how to solve it. I recommend starting with the standard model that is currently sold by Hasbro (see [www.hasbrogames.com](http://www.hasbrogames.com)) and that comes with a good set of instructions. This cube is
pretty durable and won’t easily fall apart. Later on, you might want a speed cube that is easier to turn, but these also separate into pieces more easily if you are not careful. I also recommend downloading and installing two, free software programs. The first one is called Rubik and is found at http://www.geometer.org/rubik/index.html. It will allow you to easily experiment with the cube, and then, with the click of a button, to restore it to its original configuration. The second program is called Group Explorer by Nathan Carter, and it can be found at www.platosheaven.com. You’ll also be able to find links to both of these pages at my own website, www.docbenton.com as well as instructions on how to solve Rubik’s cube. So, let the journey begin!

FACT: There are 43,252,003,274,489,856,000 permutations that can be made of the little colored squares on the faces of Rubik’s cube.

FACT: Any scrambled Rubik’s cube can, in theory, be restored to its original configuration in 20 moves or less. This number 20 is known by mathematicians and cube enthusiasts as God’s number!
1. Buy a Rubik’s cube and learn how to solve it using the solution that is posted on my web page at www.docbenton.com.

2. Download and install Rubik, and read the documentation, too. Links can be found at www.docbenton.com.

3. Download and install Group Explorer, and glance at the documentation found under the “Help” tab within the program. Links can, once again, be found at www.docbenton.com.
Our journey begins with an examination of what we mean in mathematics by a permutation, how we count permutations, and the notation that we use for permutations. This chapter has a lot of jargon and technical things in it, but it also lays the foundation for everything to follow!

**Definition:** A *permutation* of *n* objects is an arrangement in which order matters. A *combination* is an arrangement in which order doesn’t matter.

**Example 1:** Let’s let \( A = \{a,b\} \). Then we can write down the elements of this set in two different orders (in other words, two different permutations). We can write either \( ab \) or \( ba \). These represent two different permutations, but the same combination.

**Example 2:** If you are picking 5 people out of a group of 20 to serve on a committee, then the order in which the people are picked doesn’t matter. Hence, we are picking a combination of people.

**Example 3:** If you are selecting in order 3 people from a committee of 10 such that the first person picked will be the committee chair, the second person will be the vice-chair, and the third person will be the recording secretary, then the order in which the people are picked matters. Hence, we are selecting a permutation of people.
Example 4: If you are dealt a standard 5 card poker hand from a deck of 52 cards, then the order in which you are dealt the cards doesn’t matter. Thus, you have been dealt a combination of cards.

Question: Should a combination lock really be called a permutation lock?

Counting Permutations and Combinations

There is a fundamental counting principle that says that if you have a series of choices to make and if you have so many options for each choice, then the total number of possible choices is equal to the product of the number of options at each step along the way. For example, suppose you want to buy a pizza with 1 meat and 1 veggie topping, and suppose you have 3 choices for the meat, 5 for the veggie, 4 choices for the size, and 2 choices for the type of crust. Then to specify your pizza you will have to choose a meat, a veggie, a size, and a crust, and the total number of possible choices is \(3 \times 5 \times 4 \times 2 = 120\).

In general, if we want to count the number of permutations of \(n\) objects that are possible, we simply count the number of ways we can select the first object, the number of ways we can select the second object, and so on. Also, when we make these selections, we are selecting or drawing without replacement. That means that once we’ve selected an object, it’s not available to be selected again. That’s how many things in the world are selected, without replacement. The alternative is selecting with replacement which means that we can choose the same item over and over again.
Definition: The number of permutations we can make of \( n \) objects is 
\[ n(n-1)(n-2)\ldots(3)(2)(1) = n! \] (n factorial). Also, by definition we set \( 0! = 1 \). This may seem counterintuitive, but having \( 0! = 1 \) makes our standard counting formulas work out just right.

Example 5: Let’s suppose that you have 5 objects and you want to select 3 without replacement. How many permutations are possible?

The number of permutations possible is \( 5 \cdot 4 \cdot 3 = 60 \). We have 5 choices for the first object, 4 for the second, and 3 for the third. Notice that we could also write this in factorial notation as 
\[ 5 \cdot 4 \cdot 3 = \frac{5!}{2!} = \frac{5!}{(5-3)!} \]. More generally, the number of permutations of \( n \) objects where we choose \( r \) (without replacement) is 
\[ _nP_r = n(n-1)(n-2)\ldots(n-r+1) = \frac{n!}{(n-r)!} \]. Notice, too, that if we ask how many permutations of 5 objects there are if we choose all 5, then the answer is 
\[ _5P_5 = \frac{5!}{(5-5)!} = \frac{5!}{0!} = 5! \]. This is why we had to define \( 0! \) as being equal to 1.

Example 6: This time suppose that you have 5 objects and you want to select 3 without replacement. How many combinations are possible?

Let’s suppose that the objects are the letters in the set \( A = \{a, b, c, d, e\} \). Then it should be clear that the number of permutations \( _5P_3 \) over counts the number of combinations
because, for instance, \(abc\) and \(cab\) represent different permutations but the same combination. Hence, what we need to do is to figure out how many permutations we can make from letters like \(abc\), and then that will tell us by what factor we’ve over counted the number of combinations. Fortunately, that’s easy to do! The number of permutations we can make of the letters \(abc\) is \(3 \cdot 2 \cdot 1 = 3! = 6\). We can also easily list each one of these permutations as I’ve done below.

\[
\begin{align*}
abc & \quad bac & \quad cab \\
acb & \quad bca & \quad cba
\end{align*}
\]

We’ll denote the number of combinations we can make of 5 objects when we choose 3 as \(\binom{5}{3}\), and according to our discussion above, this should be equal to the number of permutations of 5 objects choose 3 divided by the number of permutations of 3 objects.

In other words, 
\[
\binom{5}{3} = \frac{5!}{3!} = \frac{(5-3)!}{3!} = 10.
\]

More generally, we have that the number of combinations of \(n\) objects choose \(r\) is 
\[
\binom{n}{r} = \frac{n!}{r!(n-r)!}.
\]

Example 7: Suppose you are ordering a pizza and you are going to select 3 different meat toppings out of 5. How many possibilities are there? The answer is given to us immediately by 
\[
\binom{5}{3} = \frac{5!}{(5-3)!3!} = 10.
\]

In this case, the order in which you select the meat toppings doesn’t matter.
Now that we know how to count things such as permutations and combinations, let’s develop some notation for denoting specific permutations. In particular, suppose \( P = \{1, 2, 3\} \). Then by a permutation of the numbers 1, 2, & 3 we mean a bijective function \( f : P \rightarrow P \). Okay, this definition probably requires a little explanation. First of all, what do we mean by a bijective function? Well, this means a function that is one-to-one and onto. The term one-to-one basically means that different elements of the domain always get paired with different elements in the range. A one-to-one function is also called injective.

**Definition:** A function \( f : D \rightarrow C \) is one-to-one (injective) if and only if for every \( a, b \in D \) with \( a \neq b \), we have that \( f(a) \neq f(b) \).

Furthermore, if \( f : D \rightarrow C \) is a function with \( f \) onto, then that means that for every \( y \in C \), there exists \( x \in D \) such that \( f(x) = y \). In other words, the range of our function is all of \( C \). Also, in notation such as the above, \( C \) is called the **codomain**. Thus, a function is onto if its range is equal to its codomain. When this happens, we also say that the function is surjective. For example, if we consider the set of natural numbers \( \mathbb{N} = \{1, 2, 3, \ldots\} \), then \( f : \mathbb{N} \rightarrow \mathbb{N} \) defined by \( f(x) = 2x \) is one-to-one, but not onto. On the other hand, if we define \( \mathbb{R}^+ = \{\text{all positive real numbers}\} \) and \( f : \mathbb{R}^+ \rightarrow \mathbb{R}^+ \) by \( f(x) = 2x \), then our function is now both one-to-one and onto.
So, having gone through all of that we can say that if \( P = \{1, 2, 3\} \), then a permutation of the elements of \( P \) corresponds to a bijective function \( f : P \to P \). One such permutation could be defined by \( f(1) = 2 \), \( f(2) = 3 \), and \( f(3) = 1 \). However, this may not be the easiest way to visualize the permutation, and so let’s explore some other notations. A notation that is a little handier is the following (along with some variations).

\[
\begin{pmatrix}
1 & 2 & 3 \\
\downarrow & \downarrow & \downarrow \\
2 & 3 & 1
\end{pmatrix}
= \begin{pmatrix}
1 & 2 & 3 \\
\downarrow & \downarrow & \downarrow \\
2 & 3 & 1
\end{pmatrix}
= \begin{pmatrix}
1 & 2 & 3 \\
\downarrow & \downarrow & \downarrow \\
2 & 3 & 1
\end{pmatrix}
\]

Another way in which we can specify a permutation is in terms of multiplication by what we call a *permutation matrix*. This is a square matrix of zeroes and ones such that each row and each column contains just a single 1. For example, below is an illustration of how to accomplish our above permutation of the numbers 1, 2, 3 by using matrix multiplication. Notice how, for instance, in order to make 2 the first number in my permutation, I have to put a 1 in the first row, second column of my square matrix, and that should be enough to explain to you how I came up with rows two and three.

\[
\begin{pmatrix}
0 & 1 & 0 \\
0 & 0 & 1 \\
1 & 0 & 0
\end{pmatrix}
\begin{pmatrix}
1 \\
2 \\
3
\end{pmatrix}
= \begin{pmatrix}
2 \\
3 \\
1
\end{pmatrix}
\]

In the long run, though, one of the most convenient notations for permutations is what is called *cycle notation*. For our permutation above the cycle notation simply looks like:
This is simply a shorthand way of saying that 1 goes to 2, 2 goes to 3, and 3 goes back to 1.

Now suppose we want a permutation such that $f(1) = 2$, $f(2) = 1$, and $f(3) = 3$. In other words, we are switching 1 and 2, but leaving 3 alone. Then this is how we could represent that permutation in each of our three notations.

\[
(1 \ 2 \ 3)
\]

(1 \ 2 \ 3)

Notice that in our cycle notation that the 3 by itself in parentheses just means that $f(3) = 3$. Usually, if an element is not being moved by our permutation, we just leave it out of our cycle notation. This allows us to write $(1 \ 2)(3)$ more simply as $(1 \ 2)$.

However, when you are first getting used to cycle notation it might help with comprehension if you write down the more complete version each time. Furthermore, a
cycle involving 3 elements is called a 3-cycle, a cycle that switches 2 elements is called a 2-cycle or *transposition*, and a cycle that leaves an element fixed is called a 1-cycle. In other words,

$$(1 \ 2 \ 3)$$ is a 3-cycle

$$(1 \ 2)$$ is a 2-cycle

$$(3)$$ is a 1-cycle

Get used to this cycle notation because that’s what we’re going to use from here on out!

If you think about it, we can multiply permutations together if by multiplication we mean “one permutation followed by another,” and when we do so, the result is another permutation. Most of the time, when we write down a product of permutations, we will proceed in order from left to right. Thus, if we want to begin with our 3-cycle above and follow it by our 2-cycle, then we can write the result in our first notation as:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

See how this works?

In the matrix notation for our permutations there are both advantages and disadvantages.

The advantage is that we can simply multiply permutation matrices together to get
another permutation matrix. The disadvantage, though, is that if we represent our first permutation matrix by \( A \) and the second by \( B \), then you would think that the product of the two permutations would be given by \( BA \) which would mean to first multiply our column matrix by \( A \) and then by \( B \). However, that doesn’t give us the correct result, but multiplying in the opposite order, \( AB \), does work, and that may seem a little strange. Nevertheless, you can verify it just by doing the multiplication yourself!

\[
BA = \begin{pmatrix}
1 & 0 & 1 & 0 & 0 \\
2 & 1 & 0 & 0 & 1 \\
3 & 0 & 0 & 1 & 0
\end{pmatrix}
= \begin{pmatrix}
0 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 \\
1 & 0 & 0 & 1 & 0
\end{pmatrix}
= \begin{pmatrix}
0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 2 & 2 \\
1 & 0 & 0 & 3 & 3
\end{pmatrix}
\begin{pmatrix}
1 \\
2 \\
3
\end{pmatrix}
= \begin{pmatrix}
3 \\
2 \\
1
\end{pmatrix}
\neq \begin{pmatrix}
1 \\
1 \\
3
\end{pmatrix}
\]

While this result may seem a little odd, it’s also advantageous in that if we are doing a permutation that begins with \( A \) and ends with \( B \), we can still write our matrices down in order from left to right just as we are doing with the other notations.

\[
AB = \begin{pmatrix}
1 & 0 & 1 & 0 & 0 \\
2 & 0 & 0 & 1 & 0 \\
3 & 1 & 0 & 0 & 1
\end{pmatrix}
= \begin{pmatrix}
0 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 \\
1 & 0 & 0 & 1 & 0
\end{pmatrix}
= \begin{pmatrix}
1 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 2 & 2 \\
0 & 1 & 0 & 3 & 3
\end{pmatrix}
\begin{pmatrix}
1 \\
1 \\
3
\end{pmatrix}
\]

And now let’s look at the product of our permutations using cycle notation, and for clarity, I’ll also write down all 1-cycles and enclose our separate permutations in brackets. Also, remember that we start on the left and work our way towards the right.
\[
\begin{bmatrix}
1 & 2 & 3 \\
\end{bmatrix} \begin{bmatrix}
1 & 2 & 3 \\
\end{bmatrix} = (1)(2)(3)
\]

The way to decipher this is as follows, and remember to read \(1 \to 2\) as “1 goes to 2.”

1 \(\to\) 2 is followed by 2 \(\to\) 1, and so 1 \(\to\) 1.

2 \(\to\) 3 is followed by 3 \(\to\) 3, and so 2 \(\to\) 3.

3 \(\to\) 1 is followed by 1 \(\to\) 2, and so 3 \(\to\) 2.

Therefore, \((1\ 2\ 3)(1\ 2) = (1)(2\ 3) = (2\ 3)\).

Notice that in a permutation such as \((1)(2\ 3)\), we have two cycles that are disjoint. That means that the cycles don’t have any elements in common, and so they don’t move anything in common. Consequently, they commute with each other which means that the order in which we write them down doesn’t make any difference.

As a final note, a permutation that merely switches two elements is called a transposition, and it turns out that any permutation can be written as a product of transpositions. However, when we do so, the cycles may not be disjoint and there is often more than one way to do it. For example, consider our 3-cycle from above.

\[
(1\ 2\ 3) = (1\ 2)(1\ 3) = (2\ 3)(2\ 1)
\]
While a representation of a permutation as a product of transpositions may not be unique, it does turn out that we will consistently wind up with either an even or an odd number of transpositions, and in this way we can classify any permutation as being either even or odd. For example, \((1 \ 2 \ 3) = (1 \ 2)(1 \ 3)\) is an even permutation, but \((1 \ 2 \ 3 \ 4) = (1 \ 2)(1 \ 3)(1 \ 4)\) is an odd permutation.

Well, now that we know everything there is to know about permutations, it’s time to count up how many permutations are possible on Rubik’s cube!
PRACTICE – PERMUTATIONS

In problems 1 through 5, assume we are talking about permutations of the numbers, 1, 2, 3, and 4.

1. Write \((1 \ 4 \ 2 \ 3)\) as a product of transpositions. Is \((1 \ 4 \ 2 \ 3)\) an even permutation or an odd permutation?

2. Write \((1 \ 4 \ 2 \ 3)\) in the form

\[
\begin{pmatrix}
1 & 2 & 3 & 4 \\
\downarrow & \downarrow & \downarrow & \downarrow \\
? & ? & ? & ?
\end{pmatrix}
\]

3. Express the permutation \((1 \ 4 \ 2 \ 3)\) as a \(4 \times 4\) permutation matrix times the column matrix

\[
\begin{pmatrix}
1 \\
2 \\
3 \\
4
\end{pmatrix}
\]

4. Multiply \((1 \ 4 \ 2 \ 3)(2 \ 3 \ 1)\). Remember to multiply left to right. Also, classify the result as either an even permutation or an odd permutation.

5. Express \((1 \ 4 \ 2 \ 3)(2 \ 3 \ 1)\) as a product of permutation matrices, and verify that it produces the correct permutation of the numbers

\[
\begin{pmatrix}
1 \\
2 \\
3 \\
4
\end{pmatrix}
\]

6. Complete the multiplication table below for the products of the permutations of the numbers 1, 2, and 3. Remember to multiply left to right.

\[
\begin{array}{ccccccc}
(1)(2)(3) & (1) & (2) & (1 \ 3) & (2 \ 3) & (1 \ 2 \ 3) & (1 \ 3 \ 2) \\
(1)(2)(3) & & & & & & \\
(1 \ 2) & & & & & & \\
(1 \ 3) & & & & & & \\
(2 \ 3) & & & & & & \\
(1 \ 2 \ 3) & & & & & & \\
(1 \ 3 \ 2) & & & & & & \\
\end{array}
\]
1. Write \((1 \ 4 \ 2 \ 3)\) as a product of transpositions. Is \((1 \ 4 \ 2 \ 3)\) an even permutation or an odd permutation?

\[(1 \ 4 \ 2 \ 3) = (1 \ 4)(1 \ 2)(1 \ 3)\] is an odd permutation.

2. Write \((1 \ 4 \ 2 \ 3)\) in the form

\[
\begin{pmatrix}
1 & 2 & 3 & 4 \\
? & ? & ? & ?
\end{pmatrix}
\]

\[
(1 \ 4 \ 2 \ 3) = \begin{pmatrix}
1 & 2 & 3 & 4 \\
? & ? & ? & ?
\end{pmatrix}
\]

3. Express the permutation \((1 \ 4 \ 2 \ 3)\) as a \(4 \times 4\) permutation matrix times the column matrix

\[
\begin{pmatrix}
1 \\
2 \\
3 \\
4
\end{pmatrix}
\]

\[
\begin{pmatrix}
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0
\end{pmatrix}
\begin{pmatrix}
1 \\
2 \\
3 \\
4
\end{pmatrix} =
\begin{pmatrix}
4 \\
3 \\
1 \\
2
\end{pmatrix}
\]

4. Multiply \((1 \ 4 \ 2 \ 3)(2 \ 3 \ 1)\). Remember to multiply left to right. Also, classify the result as either an even permutation or an odd permutation.

\[(1 \ 4 \ 2 \ 3)(2 \ 3 \ 1) = (1 \ 4 \ 3 \ 2) = (1 \ 4)(1 \ 3)(1 \ 2)\] is an odd permutation.
5. Express \((1 \ 4 \ 2 \ 3)(2 \ 3 \ 1)\) as a product of permutation matrices, and verify that it produces the correct permutation of the numbers \(1, 2, 3, 4\).

\[
\begin{pmatrix}
1 \\
2 \\
3 \\
4
\end{pmatrix}
\]

\[
(1 \ 4 \ 2 \ 3)(2 \ 3 \ 1) = \begin{pmatrix}
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0
\end{pmatrix} \begin{pmatrix}
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1
\end{pmatrix} = \begin{pmatrix}
0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0
\end{pmatrix}
\]

\[
\begin{pmatrix}
0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0
\end{pmatrix} \begin{pmatrix}
1 \\
2 \\
3 \\
4
\end{pmatrix} = \begin{pmatrix}
1 \\
1 \\
2 \\
3
\end{pmatrix}
\]

6. Complete the multiplication table below for the products of the permutations of the numbers 1, 2, and 3. Remember to multiply left to right.

<table>
<thead>
<tr>
<th></th>
<th>(1)(2)(3)</th>
<th>(1 2)</th>
<th>(1 3)</th>
<th>(2 3)</th>
<th>(1 2 3)</th>
<th>(1 3 2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)(2)(3)</td>
<td>(1)(2)(3)</td>
<td>(1 2)</td>
<td>(1 3)</td>
<td>(2 3)</td>
<td>(1 2 3)</td>
<td>(1 3 2)</td>
</tr>
<tr>
<td>(1 2)</td>
<td>(1)(2)(3)</td>
<td>(1 2)</td>
<td>(1 3)</td>
<td>(2 3)</td>
<td>(1 2 3)</td>
<td>(1 3 2)</td>
</tr>
<tr>
<td>(1 3)</td>
<td>(1 3)</td>
<td>(1 3 2)</td>
<td>(1)(2)(3)</td>
<td>(1 2 3)</td>
<td>(2 3)</td>
<td>(1 2)</td>
</tr>
<tr>
<td>(2 3)</td>
<td>(2 3)</td>
<td>(1 2 3)</td>
<td>(1 3 2)</td>
<td>(1)(2)(3)</td>
<td>(1 2)</td>
<td>(1 3)</td>
</tr>
<tr>
<td>(1 2 3)</td>
<td>(1 2 3)</td>
<td>(2 3)</td>
<td>(1 2)</td>
<td>(1 3)</td>
<td>(1 3 2)</td>
<td>(1)(2)(3)</td>
</tr>
<tr>
<td>(1 3 2)</td>
<td>(1 3 2)</td>
<td>(1 3)</td>
<td>(2 3)</td>
<td>(1 2)</td>
<td>(1)(2)(3)</td>
<td>(1 2 3)</td>
</tr>
</tbody>
</table>

By the way, notice that each row and each column contains all the possible permutations with no repetitions. As we'll see later, this is no accident!
COUNTING THE NUMBER OF PERMUTATIONS IN RUBIK’S CUBE

Below is a picture of Rubik’s cube. The surface reveals 26 smaller cubes that we’ll call “cubelets”¹ and 54 smaller faces that we’ll call “facelets.”

At first glance, you might think that the total number of permutations we can make of the facelets on Rubik’s cube is \(54! \approx 2.3 \times 10^{71}\), the number of permutations we can make of 54 things, but this is going to give us a number that is way too large. It’s too large because we can’t take a single facelet and just move it anywhere. There are going to be some restrictions on where facelets can wind up. For example, suppose we number a couple of the facelets as below.

¹ Many people also refer to “cubelets” as “cubies.”
Then there is no way that we can rotate the sides of the cube to make these numbers wind up in the following positions.
And why can’t we do this? It’s because we have three types of cubelets – center cubelets, edge cubelets, and corner cubelets. Furthermore, every time we rotate a face of the cube, the center cubelet stays where it is, an edge cubelet just gets moved to the position of another edge cubelet, and a corner cubelet gets moved to another corner. Thus, since our original numbers 1 & 2 begin on an edge and a center cubelet, respectively, they can never wind up on corner cubelets. Additionally, we’ll sometimes use notations like $UF$ and $UFR$ to refer, respectively, to the edge cubelet in the up-front position and the corner cubelet in the up-front-right position.

At this point, you might notice that the facelets of a single cubelet always have to stay together, and thus, maybe the total number of possible permutations of the facelets of Rubik’s cube will just be equal to the number of permutations of the 26 cubelets or $26! \approx 4.03 \times 10^{26}$. Well, this is still going to be too large a number because, again, there are restrictions on where you can move center, edge, and corner cubelets. As we just mentioned, every time we rotate a face, the center cubelet stays where it is, a corner cubelet replaces another corner cubelet and an edge cubelet replaces an edge cubelet. Thus, to count the actual number of possible permutations, perhaps we need to begin by multiplying the number of permutations you can make from the 8 corner cubelets times the number of permutations you can make from the 12 edge cubelets. This gives us $(8!)(12!) \approx 1.9 \times 10^{13}$. However, there are a couple of things we haven’t taken into consideration yet. One is that each corner cubelet can be rotated among three different positions, and the other is each edge cubelet can be flipped back and forth from one position to another. These rotations and flips are illustrated by the pictures below.
Thus, each of the eight corner cubelets could be in any of three rotational states, and so we should multiply our previous number by $3^8$. Similarly, since each of the twelve edge cubelets could be in either of two states, flipped or not flipped, we should also multiply our previous estimate by $2^{12}$. This will give us $(8!)(12!)(3^8)(2^{12}) \approx 5.2 \times 10^{20}$. This is smaller than our previous estimate of $26! \approx 4.03 \times 10^{26}$, but still too large, and so let’s see what we can do to reduce it.
First off, let’s number the corner cubelets 1 through 4 on the right face of the cube, and then let’s see what kind of permutation results when we rotate the right face a quarter-turn clockwise.

We can express this permutation as \((1 \ 2 \ 3 \ 4) = (1 \ 2)(1 \ 3)(1 \ 4)\), and thus, we see that it is an odd permutation since it can written as a product of three transpositions.

Now let’s number the edge cubelets 5 through 8 and do the same clockwise rotation of the right face.
We can express this result as \((5 \ 6 \ 7 \ 8) = (5 \ 6)(5 \ 7)(5 \ 8)\), and once again we get an odd permutation. However, if we now consider the permutations of the corner and edge cubelets together, then the final result of our clockwise quarter-turn is an even permutation consisting of six transpositions.

\[(1 \ 2 \ 3 \ 4)(5 \ 6 \ 7 \ 8) = (1 \ 2)(1 \ 3)(1 \ 4)(5 \ 6)(5 \ 7)(5 \ 8)\]
At this point, what this means is that every turn of a face of a cube results in an even permutation, and, hence, any combination of turns will also result in an even permutation. Thus, the number of possible permutations of the cubelets in Rubik’s cube is not \( (8!)(12!)(3^8)(2^{12}) \). Instead, it is no more than half of this, \( \frac{(8!)(12!)(3^8)(2^{12})}{2} \), since only half of the permutations represented by the number \( (8!)(12!)(3^8)(2^{12}) \) are even. However, this is still not our final answer. There are more things to consider!

To see what else we need to take into account, let’s begin with a typical representation of the coordinate axes in three dimensional space using what is known as a right-handed coordinate system.
In the diagram above, the axes are labeled on the positive side. Now let’s suppose that we attach arrows to the edge cubelets on a side of Rubik’s cube such that the arrows are pointing either in the direction of positive $x$ or positive $z$. And finally, let’s once again rotate the right face of our cube a quarter-turn in the clockwise direction, and let’s see what happens to our arrows.

The end result is that two of the arrows are now pointing in the direction of negative $x$. However, we could also say that the overall orientation is still positive since the product $(positive)(negative)(positive)(negative) = positive$. In particular, we can never wind up, after turning the face of a cube a quarter-turn, with an orientation such as $(positive)(positive)(positive)(negative) = negative$. Notice that this orientation would also correspond to a single edge cubelet being flipped.
Thus, since every quarter-turn of a face leaves us with a positive orientation, so will any combination of turns of the faces of Rubik’s cube. In particular, the number of “flipped” edge cubelets always has to be even. And as far as our problem of counting the number of permutations of Rubik’s cube goes, this means that we have to divide our last number by 2 again since only half of that number will correspond to the positive orientations of edge cubelets that we have just defined. Thus, the number of permutations that we can achieve is now no more than \[ \frac{(8!)(12!)(3^8)(2^{12})}{2 \cdot 2} \approx 1.30 \times 10^{20}. \]

There’s just one more thing we have to consider, and then we’ll be done. In particular, we need to consider how rotating a face of the cube might twist or rotate a corner cubelet. For example, below I’ve attached an arrow to top facelet of the red-yellow-blue corner cublet. If I now do a sequence of rotations of the faces of the cube such that when I’m
done the cubelet is either on the top face with arrow is pointing up or on the bottom face with the arrow pointing down, then I’ll consider the cubelet to have not been rotated.

On the other hand, if I wind up with something like the image below, then I’ll say that the cubelet has been rotated clockwise through an angle of 120°.
And finally, if I wind up with the following image, then I’ll say that my red-yellow-blue cubelet has been rotated clockwise through an angle of $240^\circ$.

And now we’re good to go! First, it should be evident that if all I do is rotate the top face or the bottom face of the cube, then none of the corner cubelets will undergo any rotation whatsoever. However, if we rotate any of the side faces (right, left, front, or back), then it’s a different story. Below I’ve placed some arrows on the corner cubelets of the right face and then rotated the right face a quarter-turn clockwise.
If we look at the corner cube that I’ve labeled 1, then it has not only been moved to a new position, it has also been rotated through an angle of $120^\circ$. In particular, the blue facelet is now on top instead of the red. Likewise, the corner cubelet labeled 2 has been moved from the top face to the bottom face, but instead of having the red facelet on the bottom, the cubelet appears to have been rotated clockwise through an angle of $240^\circ$. And similarly, we could say that the cubelet labeled 3 has been rotated clockwise through an angle of $120^\circ$, and the cubelet labeled 4 has been rotated clockwise through an angle of $240^\circ$. If we now add up total number of degrees of rotation for each of the corner cublets, it’s clear that the sum has to be either a whole number multiple of $360^\circ$ or a multiple of $360^\circ$ plus an additional $120^\circ$ or a multiple of $360^\circ$ plus an additional $240^\circ$. In the first instance, we’ll say that the cube has orientation 1, in the second case that it has orientation 2, and in the third case that it has orientation 3.

\[2\] Since cubelet 4 is now on top, a rotation of $0^\circ$ would correspond to the arrow pointing up, but instead, it’s pointing in the direction corresponding to a $240^\circ$ rotation.
Well, when we rotate the right face a quarter-turn clockwise as we did above, the sum of the angles of rotation for the corner cubelets is $120^\circ + 240^\circ + 120^\circ + 240^\circ = 720^\circ = 2 \cdot 360^\circ$. Thus, the cube is left in orientation 1. Furthermore, the sum of the sum of the angles of rotation along each side are $360^\circ$. And now, a moment’s reflection or experimentation should convince you that if you rotate any other face of the cube or any combination of faces of the cube, then the final orientation is still going to be 1. However, since there are three conceivable orientations that the cube could be left in, orientation 1 represents only a third of them, and that means that only one-third of the corner cubelet configurations that I had previously counted are actually attainable. Thus, if we divide our previous calculation by 3, then we will obtain the true number of permutations that can be made of the facelets on Rubik’s cube. The result is slightly more than forty-three quintillion.

$$\frac{(8!)(12!)(3^8)(2^{12})}{2 \cdot 2 \cdot 3} = 43,252,003,274,489,856,000 = 2^{27} \cdot 3^3 \cdot 5^3 \cdot 7^2 \cdot 11$$

Notice that if we could move any corner cubelet to any corner position and any edge cubelet to any edge position, then the correct number of possible permutations would be $(8!)(12!)(3^8)(2^{12})$. However, what we have just shown is that only a twelfth of these permutations are actually attainable. Thus, if you take your cube apart and start randomly reassembling it, then you have only a 1 in 12 chance of creating a cube that can be restored to its original configuration. And finally, how do we know that we still haven’t
overcounted the number of permutations? Simple. Because Chuck Norris has actually done all 43,252,003,274,489,856,000 permutations!³

³ Chuck Norris has also counted to infinity twice, and Chuck Norris CAN divide by zero. I, on the other hand, have only counted to infinity once, but I did start at infinity and count down.
WHAT IS A GROUP?

At this point, we’ve noticed that rotations of the faces of Rubik’s cube produce a permutation of the facelets of the cube, and we’ve learned a lot about how to both represent and multiply permutations together. If we explore a little deeper, though, we’ll discover that the permutations we can make of a set of $n$ objects will always have a very specific set of algebraic properties. We can illustrate most of them quite easily using a multiplication table that we’ve constructed for the six permutations we can make of the numbers 1, 2, 3.

\[
\begin{array}{ccccccc}
(1, 2) & (1, 2) & (1, 2) & (1, 2) & (1, 2) & (1, 2) & (1, 2) \\
(1, 3) & (1, 3) & (1, 3) & (1, 3) & (1, 3) & (1, 3) & (1, 3) \\
(2, 3) & (2, 3) & (2, 3) & (2, 3) & (2, 3) & (2, 3) & (2, 3) \\
(1, 2, 3) & (1, 2, 3) & (1, 2, 3) & (1, 2, 3) & (1, 2, 3) & (1, 2, 3) & (1, 2, 3) \\
(1, 3, 2) & (1, 3, 2) & (1, 3, 2) & (1, 3, 2) & (1, 3, 2) & (1, 3, 2) & (1, 3, 2) \\
\end{array}
\]

The first algebraic property we have is that the product of any two permutations is another permutation. We call our product a binary operation because it is a way of combining two elements in a set and getting back another element in the same set. We also call this property closure since combining the two elements doesn’t give us anything that’s not in our original set. In other words, it’s a closed system. Notice that multiplying two permutations together is a different kind of binary operation, say, than multiplying two real numbers together. Also, to specify a binary operation you have to
specify not only how the operation is performed, but also the set of elements that your
operation applies to.

The next algebraic property is the **associative property**, and this means that if \( A, B, \) and \( C \)
are any of the permutations in our above set of three numbers, then \((AB)C = A(BC)\).
This is not so easy to see from the multiplication table above, but if we think of the
multiplication of permutations as meaning “is followed by,” then we can interpret \((AB)C\)
as meaning “\((A \text{ is followed by } B) \text{ is followed by } C.\)” and we can interpret \(A(BC)\) as
meaning “\(A \text{ is followed by } (B \text{ is followed by } C).\)” Hopefully, it’s not too difficult to see
that both of these expressions simply mean “\(A \text{ is followed by } B \text{ is followed by } C.\)”

The third property is called the **identity property**. Recall that in the world of numbers we
call 0 an **additive identity** because adding it to any number doesn’t change its identity.
Likewise, 1 is a **multiplicative identity** since multiplying any number by 1 also preserves
its identity. In our table above, we can see that the **identity element** is the permutation
\((1)(2)(3)\) which leaves everything unchanged.

And our fourth and final property is called the **inverse property**. This property essentially
says that whatever you do can be undone and it should be obvious that any permutation
can reversed. Thus, from our table above we see that \((1 \ 2 \ 3)\) undoes \((1 \ 3 \ 2)\). In
other words, \((1 \ 3 \ 2)(1 \ 2 \ 3)=(1)(2)(3)\). Notice that we could also easily write the
inverse of \((1 \ 2 \ 3)\) as \((3 \ 2 \ 1)\).
We can now abstract from what we have seen happen with permutations and define a particular algebraic structure that we call a group.

**Definition:** Let $G$ be a nonempty set and let $*$ be a function with domain $G \times G$. Then the set $G$ together with the function $*$ is a group if and only if the following axioms are satisfied.

1. **(Closure)** For all $a,b \in G$, $a*b \in G$. (In other words, $*$ is function from $G \times G \to G$.)

2. **(Associativity)** For all $a,b,c \in G$, $(a*b)*c = a*(b*c)$.

3. **(Identity)** There exists an element $e$ in $G$ called the identity element with the property that for any $a \in G$, $a*e = e*a$.

4. **(Inverse)** For any $a \in G$, there exists an element $a^{-1} \in G$ with the property that $a*a^{-1} = e = a^{-1}*a$.

Any set of objects with a binary operation that satisfies these properties is called a group, and it turns out that there are many, many things in this world that are groups. The word group in many ways denotes a collection of things (like a group of friends), but in this
context it is a very special collection that also possesses these additional, algebraic properties.

Sometimes a group possesses a fifth property that we call *commutativity*, and when this happens the result is what we call either a *commutative* or *abelian group* (after the Norwegian mathematician Niels Henrik Abel (1802 – 1829) who can be said to have been one of the creators of group theory.)

5. *(Commutativity)* For all \(a, b \in G\), \(a*b = b*a\).

Usually, once a group has been defined, we just use juxtaposition to indicate the group multiplication rather than writing down “*” each time. In other words, \(a*b\) is simply replaced by \(ab\). Also, if our group is *abelian*, then it is common practice to write \(a+b\) instead of \(ab\). Additionally (no pun intended), we’ll generally denote the identity element of a group by \(e\) (or sometimes \(I\)), but for abelian groups we may also often write the identity as \(0\).

There are several reasons why groups are important in mathematics. First, they are everywhere, and that means that if you prove a general theorem about groups, then you’ve also discovered something which will be true about lots of particular cases. Second, as we will see, anytime you have either permutations or symmetry involved, then there will always be a group you can define that describes either that symmetry or set of permutations. In fact, many people see a group as something that measures the amount
of symmetry that an object has. In some fields, such as particle physics, you sometimes get to a point where all you have to work with are underlying symmetries. And lastly, note that each field of mathematics has its own area that it focuses on. For example, we might say that calculus and differential equations focus on rates of change. For group theory, however, the focus is on internal structure. As we’ll soon see, every group that we encounter may be thought of as being generated by interacting cycles and permutations, and group theory helps us to understand the internal structure of these objects as well as what is and isn’t possible.

At this point, we should probably just look at several different examples of groups so that we can appreciate just how far reaching this concept is.

1. The real numbers under addition.

2. The non-zero real numbers under multiplication.

3. The positive real numbers under multiplication.

4. The complex numbers under addition.

5. The non-zero complex numbers under multiplication.
6. The rational numbers under addition.

7. The non-zero rational numbers under multiplication.

8. The positive rational numbers under multiplication.

9. The integers under addition.

10. The integers modulo $n$ under addition (look it up, if you have to!).

11. All $3 \times 3$ invertible matrices.

12. All $3 \times 3$ permutation matrices.

13. All $3 \times 3$ orthogonal matrices. (look it up! 😊)

14. All $3 \times 3$ special orthogonal matrices. (look it up! 😊)

15. All permutations of 3 objects.

16. All quadratic polynomials in one variable with integer coefficients (the operation is addition of polynomials).
17. The group of symmetries of an equilateral triangle. By symmetries we mean those rotations about a center or flips about an axis of symmetry that preserve the distance between points and that leave the triangle looking the same as what we started with. We multiply flips and rotations by simply following one by the other.

18. The group of symmetries associated with a frieze pattern such as the one below. In this case, we see a square pattern that is repeated four times in a cycle. We also see that our basic shape has an additional mirror symmetry about a horizontal line going through its middle. Thus, we could take just the bottom half of that square and generate the whole pattern by doing translations to the right, and reflections about our axis of symmetry, and when we get to the rightmost end, we can just wrap back around to the beginning.

19. As you can see, most of the groups defined above are groups of numbers, but that is only because I am starting with what you are most familiar with. As I mentioned previously, anytime you have either permutations or symmetry involved, there’s a group lurking in the background. For example, just consider the solutions to the
quadratic equation \( ax^2 + bx + c = 0 \) that we get via the quadratic formula,

\[
x = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \quad \text{and} \quad x = \frac{-b - \sqrt{b^2 - 4ac}}{2a}.
\]

There is an obvious symmetry between these two solutions. In fact, if I define \( F \) to mean “flip the sign in front of the square root” and I define \( I \) to mean “do nothing at all,” then we get the following multiplication table for the symmetry observed here.

<table>
<thead>
<tr>
<th></th>
<th>( I )</th>
<th>( F )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( I )</td>
<td>( I )</td>
<td>( F )</td>
</tr>
<tr>
<td>( F )</td>
<td>( F )</td>
<td>( I )</td>
</tr>
</tbody>
</table>

Even though this multiplication table is pretty elementary, it does define a group. Furthermore, it was by studying such symmetries related to the solutions of polynomial equations that Evariste Galois (1811 – 1832) was able to prove that there is no general algebraic formula for solving polynomial equations of degree 5 or higher. Now that is a result that depends on group theory that is far from trivial!

The number of elements in a group \( G \) is called the \textit{order} of the group, and for the most part we will focus in this book on finite groups. Thus, if a group contains \( n \) elements, then this is denoted by writing \(|G| = n\).

Now let me show you a couple of theorems that apply to all groups, and remember, by proving these theorems for groups in general, we are simultaneously killing several
groups of birds with one stone (metaphorically, that is). This is part of the power of group theory!

**Theorem:** Let $G$ be a group. If $a, b \in G$, then $(ab)^{-1} = b^{-1}a^{-1}$.

**Proof:** To verify this, we simply need to show that $(ab)(b^{-1}a^{-1}) = e$. But this is obvious because $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$. Therefore, $(ab)^{-1} = b^{-1}a^{-1}$. □

**Theorem:** Let $G$ be a group. If $a \in G$, then $(a^{-1})^{-1} = a$.

**Proof:** Since $G$ is a group, $a^{-1}(a^{-1})^{-1} = e \Rightarrow a(a^{-1}(a^{-1})^{-1}) = ae \Rightarrow (aa^{-1})(a^{-1})^{-1} = ae \Rightarrow e(a^{-1})^{-1} = ae \Rightarrow (a^{-1})^{-1} = a$. □

---

1 We are assuming here that the inverse of a group element is unique. A proof of this is addressed in the practice exercises that follow.
PRACTICE – WHAT IS A GROUP?

1. Explain why the set of real numbers under subtraction does not form a group.
2. Explain why the set of real numbers under multiplication does not form a group.
3. Explain why the set of irrational numbers under multiplication does not form a group.
4. **Prove:** The identity element $e$ in a group $G$ is unique.
5. **Prove:** If $G$ is a group and $a \in G$, then $a$ has only one unique inverse.
1. Explain why the set of real numbers under subtraction does not form a group.

The set of real numbers under subtraction does not obey the associative law. In other words, \((3 - 2) - 1 = 1 - 1 = 0\), but \(3 - (2 - 1) = 3 - 1 = 2\). Thus, \((3 - 2) - 1 \neq 3 - (2 - 1)\).

2. Explain why the set of real numbers under multiplication does not form a group.

Because the identity in the set of real numbers under multiplication is 1, it follows that 0 is an element in this set that has no multiplicative inverse. Hence, we don’t have a group.

3. Explain why the set of irrational numbers under multiplication does not form a group.

There are two reasons this set under multiplication is not a group. First, it is not closed since \(\sqrt{2} \cdot \sqrt{2} = 2\), and 2 is not irrational, and second, the set of irrational numbers under multiplication does not contain an identity element.

4. Prove: The identity element \(e\) in a group \(G\) is unique.

**Proof:** Suppose \(e_1, e_2 \in G\) are both identity elements in a group \(G\). Then \(e_1 = e_1e_2 = e_2\).

\(\square\)

5. Prove: If \(G\) is a group and \(a \in G\), then \(a\) has only one unique inverse.

**Proof:** Suppose that \(G\) is a group and \(a \in G\) has two inverses which we’ll denote by \(a^{-1}\) and \(b^{-1}\). Then
\[
\begin{align*}
a^{-1}a &= e = b^{-1}a & \Rightarrow a^{-1}a = b^{-1}a & \Rightarrow (a^{-1}a)a^{-1} = (b^{-1}a)a^{-1} & \Rightarrow a^{-1}(aa^{-1}) = b^{-1}(aa^{-1}) \\
&\Rightarrow a^{-1}e = b^{-1}e & \Rightarrow a^{-1} = b^{-1}
\end{align*}
\]
Therefore, in a group the inverse of an element is unique. \(\square\)
In this chapter we just want to look at some very special kinds of groups, and being familiar with these groups will help us better understand all groups. The first class of groups we’ll look at are called cyclic groups.

Cyclic Groups
When we think of cyclic groups, we immediately think of clock arithmetic which is something that most people are familiar with. For example, in clock arithmetic, if you add 3 hours to 9 o’clock, then you get 12 o’clock, and if you then add 1 more hour, then you’re back at 1 o’clock. In clock arithmetic, addition causes us to cycle through the same 12 values over and over. The only change that mathematicians like to make, however, is to replace 12 by 0 since that is going to be our identity element. Thus, for mathematicians the set of elements we’ll cycle through is \{0,1,2,3,4,5,6,7,8,9,10,11\}. Furthermore, we can reach all of these elements simply by starting with 1 and repeatedly adding 1 to itself. This set, however, coupled with this type of addition results in a group, and because adding 1 to itself generates a repeating cycle, we call this a cyclic group. Furthermore, suppose we don’t have a finite cycle. In other words, suppose we can either add or subtract 1 from itself forever. In this case, we get a group that is identical to the integers, and so we denote this infinite cyclic group by \(\mathbb{Z}\), the standard symbol for the integers. On the other hand, the finite cyclic group above with only 12 elements is called
the *integers modulo* 12, and it is denoted by $\mathbb{Z}_{12}$. In this group, once we get to the 11 and add 1 to it, we start all over at 0 and repeat the cycle again.

Cyclic groups are always abelian groups, and so I’ll use additive rather than multiplicative notation for them. In particular, let’s look at the multiplication tables for $\mathbb{Z}_3$ and $\mathbb{Z}_4$.

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

*Multiplication table for $\mathbb{Z}_3$*

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

*Multiplication table for $\mathbb{Z}_4$*

One of the things we can immediately see in each table is symmetry. In other words, in both tables if you draw a line down the diagonal that starts in the upper left corner, then what is on one side of the line is a mirror image of what’s on the other side. This symmetry is a direct consequence of the fact that the groups are abelian, and you’ll find

---

1 Some mathematicians prefer the notation $C_{12}$ for this group.
this kind of symmetry in the multiplication table for any abelian group. This symmetry is an immediate consequence of equalities such as $1+2 = 2+1$.

Not only are cyclic groups very easy to understand, they are also extremely important to the deeper understanding of group theory because, as we’ll see later on, we can consider any group as being constructed from cycles or cyclic groups that interact with one another in various ways.

**Permutation Groups**

We’ve already been exposed to groups of permutations, and we’ve seen various ways to represent those permutations, and we’ve also learned how to multiply permutations. There are now just two more things we want to understand. First, if you take any set of permutations for a set of objects, and if you begin looking at all the products you can make by multiplying either those permutations or their inverses by one another, then you will generate a permutation group. Thus, permutation groups are easy to build if you are simply given a few permutations to begin with.

The second thing we want to realize is that every group is *isomorphic* to a group of permutations. The word *isomorphic* essentially means “identical shape,” and when we say that two groups are isomorphic, that means that they are essentially the same group except for how we might label the elements. In other words, the two groups have to have the same number of elements, and if $a$ and $b$ in one group are called $c$ and $d$ in the other,
then the product \( ab \) has to correspond to the product \( cd \). When two groups \( G \) and \( H \) are isomorphic, we also write \( G \cong H \).

The statement that every group is isomorphic to a permutation group is called Cayley’s Theorem after the mathematician Arthur Cayley (1821 – 1895) who discovered it. To show how this theorem works, let’s use the multiplication table for \( \mathbb{Z}_4 \) as an illustration.

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

Multiplication table for \( \mathbb{Z}_4 \)

What we want to notice is that each row of this table is also a permutation of our original set of elements \( \{0, 1, 2, 3\} \). Thus, using this table, we can establish a correspondence between elements of this group and the permutations represented by the rows. The actual correspondence for this group is shown below

\[
\begin{align*}
0 & \rightarrow (0)(1)(2)(3) \\
1 & \rightarrow (0 \ 1 \ 2 \ 3) \\
2 & \rightarrow (0 \ 2)(1 \ 3) \\
3 & \rightarrow (0 \ 3 \ 2 \ 1)
\end{align*}
\]

Furthermore, just as \( 1 + 2 = 3 \), so does \( (0 \ 1 \ 2 \ 3)(0 \ 2)(1 \ 3) = (0 \ 3 \ 2 \ 1) \).
Symmetric Groups

A special type of permutation group is the group of all permutations we can make of \( n \) objects. We call this the *symmetric group of degree* \( n \), and we denote it by \( S_n \).

Furthermore, as we’ve previously calculated, \( |S_n| = n! \). Thus, the group of permutations we can make of 3 objects is \( S_3 \), and the order or number of elements in \( S_3 \) is \( |S_3| = 3! = 3 \cdot 2 \cdot 1 = 6 \). Also, whenever we have a set of objects and a group of permutations for those objects, we like to say that the group *acts* on those objects. In more complete books on group theory, you’ll find a much more formal definition of what a *group action* is, but what I’ve said above is the essence of a group acting on a set of objects.

Dihedral Groups

The last special class of groups we want to look at are the *dihedral groups*, and these groups are going to be good examples because they involve both geometric symmetry and permutations. We’ll illustrate what a dihedral group is by looking at \( D_4 \), the dihedral group of order 8. This group is based on the isometries of a square such as the one below.
Recall that an isometry is a movement that leaves the object looking the same as what you started with and that also preserves distances between points. In the case of the square, we can either rotate it clockwise about the center through angles of $90^\circ$, or we can flip it about one of the axes of symmetry that are denoted above by the dotted lines. If we denote doing nothing to our square by $e$, a clockwise $90^\circ$ rotation by $R$, and flips about the four axes of symmetry by $F_1$, $F_2$, $F_3$, and $F_4$, then the eight elements of our group are \( \{e, R, R^2, R^3, F_1, F_2, F_3, F_4\} \). Also, the word dihedral means “two sides,” and we call these dihedral groups because, in addition to the rotations, we flip things over from one side to the other.

It’s clear that the permissible elements of this group are based upon the symmetries of the square. Furthermore, if we label our vertices 1, 2, 3, and 4, then we can keep track of how each element of the group acts upon the square, and this also shows us that each element of the group also corresponds to a particular permutation of these numbers. In particular, by examining the diagram below, you’ll be able to see how we come up with each of our permutations.
\[
\begin{align*}
e &= (1)(2)(3)(4) \\
R &= (1 \ 2 \ 3 \ 4) \\
R^2 &= (1 \ 3)(2 \ 4) \\
R^3 &= (1 \ 4 \ 3 \ 2) \\
F_1 &= (1 \ 4)(2 \ 3) \\
F_2 &= (1 \ 2)(3 \ 4) \\
F_3 &= (1 \ 3) \\
F_4 &= (2 \ 4)
\end{align*}
\]

Now notice that:

\[
\begin{align*}
F_1R &= (1 \ 4)(2 \ 3)(1 \ 2 \ 3 \ 4) = (2 \ 4) = F_4 \\
F_1R^2 &= (1 \ 4)(2 \ 3)(1 \ 3)(2 \ 4) = (1 \ 2)(3 \ 4) = F_2 \\
F_1R^3 &= (1 \ 4)(2 \ 3)(1 \ 4 \ 3 \ 2) = (1 \ 3) = F_3
\end{align*}
\]

What this last set of computations means is that every element in our dihedral group can be generated by the successive rotations combined with a single flip, and this is true for every dihedral group. Thus, when creating a multiplication table for a dihedral group, we usually express everything in terms of products of rotations and a single flip. As an illustration, we’ll examine the multiplication table for \(D_3\), the symmetries of a regular triangle.
We can write the elements of our group as \( \{e, R, R^2, F, FR, FR^2\} \). These group elements correspond to the following permutations of the labeled vertices of the triangle:

\[
\begin{align*}
 e &= (1)(2)(3) \\
 R &= (1 \ 2 \ 3) \\
 R^2 &= (1 \ 3 \ 2) \\
 F &= (2 \ 3) \\
 FR &= (1 \ 2) \\
 FR^2 &= (1 \ 3)
\end{align*}
\]

At this point, we might want to look back at the multiplication table that was presented at the beginning of our chapter on “What is a Group?”.
The table from our previous chapter is the multiplication table for the group of all permutations we can make of three objects, the group that we have now identified as $S_3$, the symmetric group of degree 3. However, this group contains the exact same permutations that are associated with $D_3$, and that means that these two groups are isomorphic. In other words, they are really the same group, just with different labels and arising from different contexts. Thus, we could just do an immediate translation of the above multiplication table into one using $F$ and $R$, but instead I want to do something a little different that winds up being a very important trick. In particular, I want you to notice that $RF = (1\ 2\ 3)(2\ 3) = (1\ 3) = FR^2$. We often call elements like $F$ and $R$ generators since we can use them to generate all the other elements in our group, and we call an equation like $RF = FR^2$ a relation because it shows us how two expressions are related to one another. This relation will also allow us to show all products in our table in terms of $F$ to a power times $R$ to a power simply by substituting $FR^2$ for any occurrence of $RF$. Thus, using this trick, here is our multiplication table. Also, even though $D_3$ and $S_3$ are isomorphic, my multiplication tables will look a little different, but that is only because the elements on the top row and side column are in a little different order.
As a final comment on dihedral groups, we denote the dihedral group associated with a regular polygon with $n$ vertices by $D_n$, and the order of $D_n$ is $|D_n| = 2n$.\(^2\)

\(^2\) Some people use the notation $D_{2n}$ instead of $D_n$. In other words, they make the subscript correspond to the order of the group instead of the number of vertices.
1. Complete the multiplication table below for $\mathbb{Z}_5$.

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2. With reference to the square diagram below, complete the following multiplication table for $D_4$.

<table>
<thead>
<tr>
<th></th>
<th>(1)(2)(3)(4)</th>
<th>(1) 2 3 4</th>
<th>(1) 3(2 4)</th>
<th>(1) 4 3 2</th>
<th>(1) 4(2) 3</th>
<th>(1) 2(3) 4</th>
<th>(1) 3 (2 4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)(2)(3)(4)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(1 2 3 4)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(1 3)(2 4)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(1 4 3 2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(1 4)(2 3)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(1 2)(3 4)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(1 3)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(2 4)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
3. With respect to the diagram below, complete the following alternate multiplication table for $D_4$.

<table>
<thead>
<tr>
<th></th>
<th>$e$</th>
<th>$R$</th>
<th>$R^2$</th>
<th>$R^3$</th>
<th>$F$</th>
<th>$FR^2$</th>
<th>$FR^3$</th>
<th>$FR$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$R$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$R^2$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$R^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$F$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$FR^2$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$FR^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$FR$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Use that,

$e = (1)(2)(3)(4)$

$R = (1\ 2\ 3\ 4)$

$R^2 = (1\ 3)(2\ 4)$

$R^3 = (1\ 4\ 3\ 2)$

$F_1 = F = (1\ 4)(2\ 3)$

$F_2 = FR^2 = (1\ 2)(3\ 4)$

$F_3 = FR^3 = (1\ 3)$

$F_4 = FR = (2\ 4)$

$FR = R^3F$ & $RF = FR^3$
1. Complete the multiplication table below for $\mathbb{Z}_5$.

\[
\begin{array}{c|ccccc}
  & 0 & 1 & 2 & 3 & 4 \\
\hline
0 & 0 & 1 & 2 & 3 & 4 \\
1 & 1 & 2 & 3 & 4 & 0 \\
2 & 2 & 3 & 4 & 0 & 1 \\
3 & 3 & 4 & 0 & 1 & 2 \\
4 & 4 & 0 & 1 & 2 & 3 \\
\end{array}
\]
2. With reference to the square diagram below, complete the following multiplication table for $D_4$.

<table>
<thead>
<tr>
<th></th>
<th>(1)(2)(3)(4)</th>
<th>(1 2 3 4)</th>
<th>(1 3)(2 4)</th>
<th>(1 4 3 2)</th>
<th>(1 4)(2 3)</th>
<th>(1 2)(3 4)</th>
<th>(1 3)</th>
<th>(2 4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)(2)(3)(4)</td>
<td>(1)(2)(3)(4)</td>
<td>(1 2 3 4)</td>
<td>(1 3)(2 4)</td>
<td>(1 4 3 2)</td>
<td>(1 4)(2 3)</td>
<td>(1 2)(3 4)</td>
<td>(1 3)</td>
<td>(2 4)</td>
</tr>
<tr>
<td>(1 2 3 4)</td>
<td>(1 2 3 4)</td>
<td>(1 3)(2 4)</td>
<td>(1 4 3 2)</td>
<td>(1)(2)(3)(4)</td>
<td>(1 3)</td>
<td>(2 4)</td>
<td>(1 2)(3 4)</td>
<td>(1 4)(2 3)</td>
</tr>
<tr>
<td>(1 3)(2 4)</td>
<td>(1 3)(2 4)</td>
<td>(1 4 3 2)</td>
<td>(1)(2)(3)(4)</td>
<td>(1 2 3 4)</td>
<td>(1 2)(3 4)</td>
<td>(1 4)(2 3)</td>
<td>(2 4)</td>
<td>(1 3)</td>
</tr>
<tr>
<td>(1 4 3 2)</td>
<td>(1 4 3 2)</td>
<td>(1)(2)(3)(4)</td>
<td>(1 2 3 4)</td>
<td>(1 3)(2 4)</td>
<td>(2 4)</td>
<td>(1 3)</td>
<td>(1 4)(2 3)</td>
<td>(1 2)(3 4)</td>
</tr>
<tr>
<td>(1 4)(2 3)</td>
<td>(1 4)(2 3)</td>
<td>(2 4)</td>
<td>(1 2)(3 4)</td>
<td>(1 3)</td>
<td>(1)(2)(3)(4)</td>
<td>(1 3)(2 4)</td>
<td>(1 4 3 2)</td>
<td>(1 2 3 4)</td>
</tr>
<tr>
<td>(1 2)(3 4)</td>
<td>(1 2)(3 4)</td>
<td>(1 3)</td>
<td>(1 4)(2 3)</td>
<td>(2 4)</td>
<td>(1 3)(2 4)</td>
<td>(1)(2)(3)(4)</td>
<td>(1 2 3 4)</td>
<td>(1 4 3 2)</td>
</tr>
<tr>
<td>(1 3)</td>
<td>(1 3)</td>
<td>(1 4)(2 3)</td>
<td>(2 4)</td>
<td>(1 2)(3 4)</td>
<td>(1 2 3 4)</td>
<td>(1 4 3 2)</td>
<td>(1)(2)(3)(4)</td>
<td>(1 3)(2 4)</td>
</tr>
<tr>
<td>(2 4)</td>
<td>(2 4)</td>
<td>(1 2)(3 4)</td>
<td>(1 3)</td>
<td>(1 4)(2 3)</td>
<td>(1 4 3 2)</td>
<td>(1 2 3 4)</td>
<td>(1 3)(2 4)</td>
<td>(1)(2)(3)(4)</td>
</tr>
</tbody>
</table>
3. With respect to the diagram below, complete the following alternate multiplication table for $D_4$.

<table>
<thead>
<tr>
<th></th>
<th>$e$</th>
<th>$R$</th>
<th>$R^2$</th>
<th>$R^3$</th>
<th>$F$</th>
<th>$FR^2$</th>
<th>$FR^3$</th>
<th>$FR$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e$</td>
<td>$e$</td>
<td>$R$</td>
<td>$R^2$</td>
<td>$R^3$</td>
<td>$F$</td>
<td>$FR^2$</td>
<td>$FR^3$</td>
<td>$FR$</td>
</tr>
<tr>
<td>$R$</td>
<td>$R$</td>
<td>$R^2$</td>
<td>$R^3$</td>
<td>$e$</td>
<td>$FR^3$</td>
<td>$FR$</td>
<td>$FR^2$</td>
<td>$F$</td>
</tr>
<tr>
<td>$R^2$</td>
<td>$R^2$</td>
<td>$R^3$</td>
<td>$e$</td>
<td>$R$</td>
<td>$FR^2$</td>
<td>$F$</td>
<td>$FR$</td>
<td>$FR^3$</td>
</tr>
<tr>
<td>$R^3$</td>
<td>$R^3$</td>
<td>$e$</td>
<td>$R$</td>
<td>$R^2$</td>
<td>$FR$</td>
<td>$FR^3$</td>
<td>$F$</td>
<td>$FR^2$</td>
</tr>
<tr>
<td>$F$</td>
<td>$F$</td>
<td>$FR$</td>
<td>$FR^2$</td>
<td>$FR^3$</td>
<td>$e$</td>
<td>$R^2$</td>
<td>$R^3$</td>
<td>$R$</td>
</tr>
<tr>
<td>$FR^2$</td>
<td>$FR^2$</td>
<td>$FR^3$</td>
<td>$F$</td>
<td>$FR$</td>
<td>$R^2$</td>
<td>$e$</td>
<td>$R$</td>
<td>$R^3$</td>
</tr>
<tr>
<td>$FR^3$</td>
<td>$FR^3$</td>
<td>$F$</td>
<td>$FR$</td>
<td>$FR^2$</td>
<td>$R$</td>
<td>$R^3$</td>
<td>$e$</td>
<td>$R^2$</td>
</tr>
<tr>
<td>$FR$</td>
<td>$FR$</td>
<td>$FR^2$</td>
<td>$FR^3$</td>
<td>$F$</td>
<td>$R^3$</td>
<td>$R$</td>
<td>$R^2$</td>
<td>$e$</td>
</tr>
</tbody>
</table>

Use that,

- $e = (1)(2)(3)(4)$
- $R = (1\ 2\ 3\ 4)$
- $R^2 = (1\ 3)(2\ 4)$
- $R^3 = (1\ 4\ 3\ 2)$
- $F_1 = F = (1\ 4)(2\ 3)$
- $F_2 = FR^2 = (1\ 2)(3\ 4)$
- $F_3 = FR^3 = (1\ 3)$
- $F_4 = FR = (2\ 4)$
- $FR = R^3 F$ & $RF = FR^3$
Let’s take another look at the structure of $S_3$, the symmetric group of degree 3, and recall that this group is isomorphic to $D_3$, the dihedral group that describes the symmetries to be found in an equilateral triangle. For convenience, below is the multiplication table for $D_3$ that we constructed at the end of the last chapter.

<table>
<thead>
<tr>
<th></th>
<th>$e$</th>
<th>$R$</th>
<th>$R^2$</th>
<th>$F$</th>
<th>$FR$</th>
<th>$FR^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e$</td>
<td>$e$</td>
<td>$R$</td>
<td>$R^2$</td>
<td>$F$</td>
<td>$FR$</td>
<td>$FR^2$</td>
</tr>
<tr>
<td>$R$</td>
<td>$R$</td>
<td>$R^2$</td>
<td>$e$</td>
<td>$FR^2$</td>
<td>$F$</td>
<td>$FR$</td>
</tr>
<tr>
<td>$R^2$</td>
<td>$R^2$</td>
<td>$e$</td>
<td>$R$</td>
<td>$FR$</td>
<td>$FR^2$</td>
<td>$F$</td>
</tr>
<tr>
<td>$F$</td>
<td>$F$</td>
<td>$FR$</td>
<td>$FR^2$</td>
<td>$e$</td>
<td>$R$</td>
<td>$R^2$</td>
</tr>
<tr>
<td>$FR$</td>
<td>$FR$</td>
<td>$FR^2$</td>
<td>$F$</td>
<td>$R^2$</td>
<td>$e$</td>
<td>$R$</td>
</tr>
<tr>
<td>$FR^2$</td>
<td>$FR^2$</td>
<td>$F$</td>
<td>$FR$</td>
<td>$R$</td>
<td>$R^2$</td>
<td>$e$</td>
</tr>
</tbody>
</table>

Now 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. 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 $h_1h_2 \in H$ (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.

\[
\begin{align*}
\{e\},
\{e, R\},
\{e, R^2\},
\{e, FR\},
\{e, FR^2\},
\{e, R, R^2, F, FR, FR^2\}
\end{align*}
\]

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*.

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 $H \cap aH = \emptyset$. 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 $H = \{e, R, R^2\}$. We basically are going to have two left cosets which we can denote as follows.

\[
eH = H = \begin{cases} e \\ R \\ R^2 \end{cases}, FH = \begin{cases} F \\ FR \\ FR^2 \end{cases}
\]

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 cosets 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. We’ll state it as
follows.

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:

$$H = \begin{cases} e \end{cases}, RH = \begin{cases} R \end{cases}, R^2H = \begin{cases} R^2 \end{cases}$$
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.

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

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

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

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

$$RH = \left\{ \frac{R}{F} \right\} \neq \left\{ \frac{R}{F} \right\} = HR$$

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 \(S_3\) from the last chapter.

<table>
<thead>
<tr>
<th></th>
<th>(1)(2)(3)</th>
<th>(1 2)</th>
<th>(1 3)</th>
<th>(2 3)</th>
<th>(1 2 3)</th>
<th>(1 3 2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)(2)(3)</td>
<td>(1)(2)(3)</td>
<td>(1 2)</td>
<td>(1 3)</td>
<td>(2 3)</td>
<td>(1 2 3)</td>
<td>(1 3 2)</td>
</tr>
<tr>
<td>(1 2)</td>
<td>(1 2)</td>
<td>(1)(2)(3)</td>
<td>(1 2 3)</td>
<td>(1 3 2)</td>
<td>(1 3)</td>
<td>(2 3)</td>
</tr>
<tr>
<td>(1 3)</td>
<td>(1 3)</td>
<td>(1 3 2)</td>
<td>(1)(2)(3)</td>
<td>(1 2 3)</td>
<td>(2 3)</td>
<td>(1 2)</td>
</tr>
<tr>
<td>(2 3)</td>
<td>(2 3)</td>
<td>(1 2 3)</td>
<td>(1 3 2)</td>
<td>(1)(2)(3)</td>
<td>(1 2)</td>
<td>(1 3)</td>
</tr>
<tr>
<td>(1 2 3)</td>
<td>(1 2 3)</td>
<td>(2 3)</td>
<td>(1 2)</td>
<td>(1 3)</td>
<td>(1 3 2)</td>
<td>(1)(2)(3)</td>
</tr>
<tr>
<td>(1 3 2)</td>
<td>(1 3 2)</td>
<td>(1 3)</td>
<td>(2 3)</td>
<td>(1 2)</td>
<td>(1)(2)(3)</td>
<td>(1 2 3)</td>
</tr>
</tbody>
</table>

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, \((1 2)^3 = (1)(2)(3)\) and
\((1 \ 2 \ 3)^3 = (1)(2)(3)\). 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 \((a \ b)(c \ d \ e)\), then we also have by direct multiplication of cycles that 
\[
[(a \ b)(c \ d \ e)]^3 = (a \ b)^3 (c \ d \ e)^3 = (a \ b)^3 = (a \ b)^2 (a \ b) = (a \ b).
\]
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 \(aH^{-1}a^{-1} = H\). 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 permutations or an odd number of permutations. 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 $\mathbb{Z}_{12} \cong \mathbb{Z}_4 \oplus \mathbb{Z}_3$. 
1. The group of symmetries of the equilateral triangle, $S_3$, has six subgroups, one of which is the trivial subgroup $\{e\}$ and another is the whole group itself. Use the multiplication table below to find the remaining four subgroups.

<table>
<thead>
<tr>
<th></th>
<th>(1)(2)(3)</th>
<th>(1 2)</th>
<th>(1 3)</th>
<th>(2 3)</th>
<th>(1 2 3)</th>
<th>(1 3 2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)(2)(3)</td>
<td>(1)(2)(3)</td>
<td>(1 2)</td>
<td>(1 3)</td>
<td>(2 3)</td>
<td>(1 2 3)</td>
<td>(1 3 2)</td>
</tr>
<tr>
<td>(1 2)</td>
<td>(1 2)</td>
<td>(1)(2)(3)</td>
<td>(1 2 3)</td>
<td>(1 3 2)</td>
<td>(1 3)</td>
<td>(2 3)</td>
</tr>
<tr>
<td>(1 3)</td>
<td>(1 3)</td>
<td>(1 3 2)</td>
<td>(1)(2)(3)</td>
<td>(1 2 3)</td>
<td>(2 3)</td>
<td>(1 2)</td>
</tr>
<tr>
<td>(2 3)</td>
<td>(2 3)</td>
<td>(1 2 3)</td>
<td>(1 3 2)</td>
<td>(1)(2)(3)</td>
<td>(1 2)</td>
<td>(1 3)</td>
</tr>
<tr>
<td>(1 2 3)</td>
<td>(1 2 3)</td>
<td>(2 3)</td>
<td>(1 2)</td>
<td>(1 3)</td>
<td>(1 3 2)</td>
<td>(1)(2)(3)</td>
</tr>
<tr>
<td>(1 3 2)</td>
<td>(1 3 2)</td>
<td>(1 3)</td>
<td>(2 3)</td>
<td>(1 2)</td>
<td>(1)(2)(3)</td>
<td>(1 2 3)</td>
</tr>
</tbody>
</table>

2. For each subgroup of order 2 or 3 in $S_3$, find the left coset created by multiplying the subgroup on the left by the permutation $(1 2 3)$.

3. **Prove:** $S_3$ has no subgroup of order 5.

4. **Prove:** For any group $G$, $\{e\}$ is a normal subgroup.
1. The group of symmetries of the equilateral triangle, $S_3$, has six subgroups, one of which is the trivial subgroup $\{e\}$ and another is the whole group itself. Use the multiplication table below to find the remaining four subgroups.

\[
\begin{array}{ccccccc}
(1)(2)(3) & (1)(2)(3) & (1) & (2) & (1) & (3) & (2) & (3) \\
(1) & (2) & (1)(2)(3) & (123) & (123) & (23) & (12) & (13) \\
(1) & (3) & (1) & (3) & (1)(2)(3) & (123) & (23) & (12) \\
(2) & (3) & (2) & (3) & (1)(2)(3) & (123) & (23) & (12) \\
(1) & (2) & (123) & (123) & (23) & (13) & (23) & (13) \\
(1) & (3) & (1) & (3) & (13) & (23) & (12) & (13) \\
(2) & (3) & (2) & (3) & (23) & (13) & (23) & (13) \\
(3) & (2) & (2) & (3) & (13) & (23) & (12) & (13) \\
\end{array}
\]

The remaining subgroups are $\left\{ (1)(2)(3) \right\}$, $\left\{ (1) \right\}$, $\left\{ (3) \right\}$, and $\left\{ (2) \right\}$.
2. For each subgroup of order 2 or 3 in \( S_3 \), find the left coset created by multiplying the subgroup on the left by the permutation \((1 \ 2 \ 3)\).

\[
\begin{align*}
\begin{pmatrix} 1 & 2 & 3 \\
1 & 2 & 3 \\
(1 & 2 & 3)
\end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\
1 & 2 & 3 \\
(1 & 2 & 3)
\end{pmatrix} &= \begin{pmatrix} 1 & 2 & 3 \\
2 & 3 & 1 \\
(2 & 3 & 1)
\end{pmatrix} \\
\begin{pmatrix} 1 & 2 & 3 \\
1 & 2 & 3 \\
(1 & 3 & 2)
\end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\
1 & 2 & 3 \\
(1 & 3 & 2)
\end{pmatrix} &= \begin{pmatrix} 1 & 2 & 3 \\
1 & 2 & 3 \\
(1 & 3 & 2)
\end{pmatrix} \\
\begin{pmatrix} 1 & 2 & 3 \\
2 & 3 & 1 \\
(2 & 3 & 1)
\end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\
2 & 3 & 1 \\
(2 & 3 & 1)
\end{pmatrix} &= \begin{pmatrix} 1 & 2 & 3 \\
1 & 3 & 2 \\
(1 & 3 & 2)
\end{pmatrix} \\
\begin{pmatrix} 1 & 2 & 3 \\
2 & 3 & 1 \\
(2 & 3 & 1)
\end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\
1 & 2 & 3 \\
(1 & 3 & 2)
\end{pmatrix} &= \begin{pmatrix} 1 & 2 & 3 \\
1 & 3 & 2 \\
(1 & 3 & 2)
\end{pmatrix} \\
\begin{pmatrix} 1 & 2 & 3 \\
1 & 2 & 3 \\
(1 & 3 & 2)
\end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\
2 & 3 & 1 \\
(2 & 3 & 1)
\end{pmatrix} &= \begin{pmatrix} 1 & 2 & 3 \\
1 & 3 & 2 \\
(1 & 3 & 2)
\end{pmatrix}
\end{align*}
\]

3. \textbf{Prove:} \( S_3 \) has no subgroup of order 5.

\textbf{Proof:} The order of \( S_3 \) is \( |S_3| = 3! = 6 \), and 5 is not a divisor of 6. Hence, by Lagrange’s Theorem, \( S_3 \) cannot have a subgroup of order 5. \( \square \)

4. \textbf{Prove:} For any group \( G \), \( \{e\} \) is a normal subgroup.

\textbf{Proof:} Let \( G \) be a group and let \( a \in G \). Then \( aea^{-1} = aa^{-1} = e \in \{e\} \). Therefore, \( \{e\} \) is a normal subgroup of \( G \), \( \{e\} \triangleleft G \). \( \square \)
RUBIK’S CUBE SUBGROUPS

The tools that we developed in the previous chapter can now give us more information about the kinds of subgroups that exist within all the permutations that may be reached on Rubik’s cube. For example, we previously showed that the total number of attainable permutations is 43,252,003,274,489,856,000. This rather large number factors into $2^{27} \cdot 3^{14} \cdot 5^3 \cdot 7^2 \cdot 11$. This immediately tells us several things. For instance, there will be Sylow $p$-subgroups with orders of $2^{27}$, $3^{14}$, $5^3$, $7^2$, and 11. In fact, here is a generator for one of the Sylow 11-subgroups. Interesting, isn’t it!

$$U^{-1}FBU^{-1}F^{-1}DBUD^{-1}U^{-1}RRD^{-1}LLU^{-1}LLD^{-1}LLU^{-1}R$$

There will be additional subgroups of orders 2, 3, 5, and 7 raised to all the various powers between 1 and the power of the corresponding Sylow $p$-subgroup. And then there will undoubtedly be a whole lot of other subgroups whose orders are not simply a prime raised to a power. However, we know immediately that there is no subgroup of order 13. And how do we know this? Simple! It’s because 13 doesn’t divide the order of the group.

The cube group itself is generated by the operations of $R$, $L$, $U$, $D$, $F$, and $B$ being applied to the cube, and each individual operation generates a cyclic group of order 4. For example, $\langle R \rangle = \{e, R, R^2, R^3\}$ is the subgroup that we generate by rotating the right face of
the cube a quarter turn each time, and this subgroup is isomorphic to \( \mathbb{Z}_4 \). Likewise, \( \langle L \rangle \), \( \langle U \rangle \), \( \langle D \rangle \), \( \langle F \rangle \), and \( \langle B \rangle \) are all isomorphic to \( \mathbb{Z}_4 \).

However, if we look at the subgroup that is generated by both \( R \) and \( L \), i.e. by twisting the right and left faces separately, then since these operations commute with one another we get \( \langle R, L \rangle \cong \mathbb{Z}_4 \oplus \mathbb{Z}_4 \). In other words, we can think of the group that is generated by \( R \) and \( L \) as simply consisting of ordered pairs where the elements of \( R \) might occupy the first coordinate, and then the elements of \( L \) can occupy the second coordinate. It’s a nice, simple, abelian group. However, if we perform the move \( RU \) on the cube, then we are working with cycles that overlap, and the result is far from abelian, or, to put it another way, \( RU \neq UR \). Furthermore, if we keep repeating this move \( RU \), then we eventually generate a cyclic group of order 105!
$RU \neq UR$

Things work out a little differently, though, if we repeatedly do the operation $R^2U^2$. For one thing, if we look at the cycle structure of just the permuted cublets and ignore any rotations or flips that might occur along the way, then we can describe it by

$$(UB \ UF)(BR \ FR)(UL \ UR \ DR)(UBL \ UFR \ DBR)(ULF \ URB \ DRF).$$
Notice that we have two cycles of length 2 and three cycles of length 3. This means that if we do this operation twice, \((R^2U^2)^2\), then we will undo the 2-cycles and just be left with some 3-cycles. In fact, the resulting permutation is

\[
(DR\; UR\; UL)(DBR\; UFR\; UBL)(DRF\; URB\; ULF).
\]

To see this algebraically, let’s just raise our first permutation to the second power. If we do, then we’ll get

\[
\left[(UB\; UF)(BR\; FR)(UL\; UR\; DR)(UBL\; UFR\; DBR)(ULF\; URB\; DRF)\right]^2
\]

\[
= (UB\; UF)^2 \; (BR\; FR)^2 \; (UL\; UR\; DR)^2 \; (UBL\; UFR\; DBR)^2 \; (ULF\; URB\; DRF)^2
\]

\[
= (UL\; UR\; DR)^2 \; (UBL\; UFR\; DBR)^2 \; (ULF\; URB\; DRF)^2
\]

\[
= (DR\; UR\; UL)(DBR\; UFR\; UBL)(DRF\; URB\; ULF).
\]

Any questions? If we look more closely at the resulting permutation, we see that it cycles three edge cubelets and also cycles two different sets of corner cubelets. In particular, the down-right, up-right, and up-left cubelets will cycle amongst themselves.
If we cube $R^2U^2$, however, then we’ll get rid of the 3-cycles and we’ll be left with only a couple of 2-cycles. Algebraically, the result is

\[
(R^2U^2)^3 = [(UB\ UF)(BR\ FR)(UL\ UR\ DR)(UBL\ UFR\ DBR)(ULF\ URB\ DRF)]^3 \\
= (UB\ UF)^3 (BR\ FR)^3 (UL\ UR\ DR)^3 (UBL\ UFR\ DBR)^3 (ULF\ URB\ DRF)^3 \\
= (UB\ UF)(BR\ FR).
\]
This final result looks particularly useful because essentially we are just swapping two back cubelets for two front cubelets, and if you try this move, then you’ll get a very nice and elegant pattern. And lastly, since $R^2U^2$ results in a combination of 2-cycles and 3-cycles, it follows that if we perform this operation six times, then all the cubelets will be restored to their original positions. When we try it, that is indeed what happens, and fortunately the orientations of the cubelets are also restored. Thus, the order of the cyclic group generated by $R^2U^2$ is six. In symbols, we write $\left|\langle R^2U^2 \rangle \right| = 6$. One of the very important lessons from this example, however, is that looking at the cycle structure of a permutation can help us determine not only the order of the corresponding cyclic group, but also what powers of this permutation might result in moving only a minimum number of cubelets in our Rubik’s cube.

And finally, if we look at not only the cyclic group generated by $R^2U^2$, but also the group generated by $R^2$ and $U^2$ (denoted by $\langle R^2,U^2 \rangle$) acting either together or independently, then it turns out that this group is isomorphic to $D_6$, the symmetries of a regular hexagon. This is also an example of what on the cube we call a two-squares group.

Another subgroup of the cube group that is both simple and interesting is called the slice group. This subgroup is generated by rotating only the center slices, and as such, it will leave the corners of the cube untouched. Consequently, this group can be used to create some pretty patterns. Also, since it is not always easy to rotate a middle slice, we can
accomplish the same effect by performing $RL^{-1}$, $FB^{-1}$, and $UD^{-1}$. Thus, the slice group is generated by these elements, $\langle RL^{-1}, FB^{-1}, UD^{-1} \rangle$.

Also interesting and mathematically simpler is the slice-squared group,

$$\langle (RL^{-1})^2, (FB^{-1})^2, (UD^{-1})^2 \rangle = \langle R^2 L^2, F^2 B^2, U^2 D^2 \rangle = \langle R^2 L^2, F^2 B^2, U^2 D^2 \rangle.$$
This group consists of eight elements, and it’s abelian. And that means, by the 
Fundamental Theorem of Finite Abelian Groups, there are only three possibilities for the 
structure of the slice-squared group. It has to be isomorphic to either $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, or 
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. See if you can figure out what the correct answer is!

And finally, I want to talk about just one more group that I can associate with Rubik’s 
cube. This is going to be the group generated by rotating the whole cube clockwise with 
respect to either the up face, the right face, or the front face. I’ll represent quarter turns in 
each of these directions by $U$, $R$, and $F$. Since these moves create a permutation of the 
six faces of the cube, the group generated has to be some subgroup of $S_6$ which has order 
$6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720$. However, we won’t get $S_6$ in its entirety. In fact, I claim that our 
subgroup will only have order 24. To see this, notice that we have six choices we could 
make regarding which colored face to have at the top of our cube. However, once we 
have picked a top color, then we have four choices for the front color, and once we have 
made these two choices, then we’re done. Those two choices will establish a particular 
arrrangement for the six faces of the cube. Thus, the total number of arrangements we can 
have is $6 \cdot 4 = 24$. Another way to look at this is to construct the four possible diagonals 
that can go from a bottom corner of the cube to a top corner of the cube, and let’s suppose 
we give each diagonal a different color, such as red, blue, orange, or magenta.
Then every turn of the cube by \( U, R, \) or \( F \) will produce some permutation of these four diagonals, and the total number of permutations possible is \( 4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24 \). Furthermore, notice that \( U^{-1}RU \) is equivalent to \( F \). Thus, we could generate this group using only \( U \) and \( R \), but it’s conceptually easier to think of it as being generated by \( U, R, \) and \( F \). Also, no one has named this particular group, and so I recommend calling it **Benton’s Group.** (Hey! I need the fame!) And lastly, since \( |S_4| = 24 \), it turns out that **Benton’s Group** is isomorphic to \( S_4 \). Sweet!
Benton’s Group $\cong S_4$

$|S_4| = 24$

(Make me famous!)
CONJUGATES AND COMMUTATORS

If $G$ is a group, and $x, a \in G$, then the element $axa^{-1}$ is called a *conjugate* of $x$. Additionally, if $H$ is a subgroup of $G, H \leq G$, then we can define the conjugate of the whole subgroup as $aH a^{-1} = \{axa^{-1} | x \in H \}$. And now we claim that if $H$ is a subgroup of $G$, then so is $aH a^{-1}$. We’ll prove this is the case just for finite groups since that is our primary interest.

**Theorem:** If $G$ is a finite group, $H$ is a subgroup of $G$, and $a \in G$, then $aH a^{-1}$ is also a subgroup of $G$.

**Proof:** Since $G$ is a finite group, it suffices to show that $aH a^{-1}$ is closed under multiplication. Thus, suppose that $b, c \in aH a^{-1}$. Then there exist $x$ and $y$ in $H$ such that $b = axa^{-1}$ and $c = aya^{-1}$. Hence, $bc = (axa^{-1})(aya^{-1}) = a(xy)a^{-1} \in aH a^{-1}$ since $xy \in H$.

Therefore, $aH a^{-1}$ is a subgroup of $G$. □

We’ve mentioned previously that some subgroups have the special property that $aH a^{-1} = H$ for all $a \in G$, and when this happens, we say that the subgroup is a normal subgroup and write $H \triangleleft G$. What our theorem above shows is that even if $aH a^{-1} \neq H$, then $aH a^{-1}$ will still be a subgroup of $G$. Also, if the only normal subgroups of a group $G$ are $G$ and $\{e\}$, then we call $G$ a *simple group*. 
Recall now our earlier discussion of Sylow $p$-subgroups where our theorem said that if $p^n$ is the highest power of a prime $p$ that divides into the order of our group $G$, then $G$ will have a subgroup of order $p^n$, a Sylow p-subgroup. We’ll now state our second and third Sylow Theorems.

The Second Sylow Theorem: Let $G$ be a finite group, and let $p$ be a prime that divides the order of $G$. Then all Sylow $p$-subgroups of $G$ are conjugate to one another.

The Third Sylow Theorem: The number of Sylow $p$-subgroups of a finite group $G$ is a divisor of the order of $G$.

Hence, from this it follows that if our Sylow $p$-subgroup is not normal, then we can find all of the Sylow $p$-subgroups just by taking conjugates of a single Sylow $p$-subgroup. If we go back to our multiplication table for $S_3$, we can easily verify that all the subgroups of order 2 are conjugate.

<table>
<thead>
<tr>
<th></th>
<th>(1)(2)(3)</th>
<th>(1 2)</th>
<th>(1 3)</th>
<th>(2 3)</th>
<th>(1 2 3)</th>
<th>(1 3 2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)(2)(3)</td>
<td>(1)(2)(3)</td>
<td>(1 2)</td>
<td>(1 3)</td>
<td>(2 3)</td>
<td>(1 2 3)</td>
<td>(1 3 2)</td>
</tr>
<tr>
<td>(1 2)</td>
<td>(1 2)</td>
<td>(1)(2)(3)</td>
<td>(1 2 3)</td>
<td>(1 3 2)</td>
<td>(1 3)</td>
<td>(2 3)</td>
</tr>
<tr>
<td>(1 3)</td>
<td>(1 3)</td>
<td>(1 3 2)</td>
<td>(1)(2)(3)</td>
<td>(1 2 3)</td>
<td>(2 3)</td>
<td>(1 2)</td>
</tr>
<tr>
<td>(2 3)</td>
<td>(2 3)</td>
<td>(1 2 3)</td>
<td>(1 3 2)</td>
<td>(1)(2)(3)</td>
<td>(1 2)</td>
<td>(1 3)</td>
</tr>
<tr>
<td>(1 2 3)</td>
<td>(1 2 3)</td>
<td>(2 3)</td>
<td>(1 2)</td>
<td>(1 3)</td>
<td>(1 3 2)</td>
<td>(1)(2)(3)</td>
</tr>
<tr>
<td>(1 3 2)</td>
<td>(1 3 2)</td>
<td>(1 3)</td>
<td>(2 3)</td>
<td>(1 2)</td>
<td>(1)(2)(3)</td>
<td>(1 2 3)</td>
</tr>
</tbody>
</table>
For example, we have three subgroups of order 2. Namely, $\{(1)(2)(3)\}$, $\{(1)(2)(3)\}$, and $\{(1)(2)(3)\}$. If we now create some conjugates by multiplying $\{(1)(2)(3)\}$ by $(1\ 3)$ and $(2\ 3)$ [Note that each of these elements is its own inverse], then we obtain:

$$(1\ 3)\{(1)(2)(3)\}(1\ 3) = \{(1)(2)(3)\} \quad \text{and} \quad (2\ 3)\{(1)(2)(3)\}(2\ 3) = \{(1)(2)(3)\}.$$ 

Thus, the other two groups are conjugate to the first, and hence, they are all conjugate to each other.

The second concept we want to look at is that of a commutator. Basically, if $x, y \in G$, then the *commutator* of $x$ and $y$ is the product $xyx^{-1}y^{-1}$. Notice that if $G$ is an abelian group or if $x$ and $y$ commute with one another, then $xyx^{-1}y^{-1} = xx^{-1}yy^{-1} = e$, the identity element in $G$. On the other hand, if $x$ and $y$ don’t commute with one another, but if their corresponding permutations don’t have much in common, then their commutator probably won’t result in too many changes. For example, let’s suppose that $X = (1\ 2\ 3)(4\ 5\ 6)$ and $Y = (6\ 7\ 8)(9\ 10)$. Then $X^{-1} = (6\ 5\ 4)(3\ 2\ 1)$ and $Y^{-1} = (10\ 9)(8\ 7\ 6)$. The only item both $X$ and $Y$ permute is 6, and their commutator is,

$$XYX^{-1}Y^{-1} = (1\ 2\ 3)(4\ 5\ 6)(6\ 7\ 8)(9\ 10)(6\ 5\ 4)(3\ 2\ 1)(10\ 9)(8\ 7\ 6) = (5\ 6\ 8)$$
Thus, even though our permutations don’t commute, the commutator still undoes quite a bit of what gets moved around.

Now let’s suppose that we take all the commutators in our group and form all possible, finite products with them. This will generate a subgroup of $G$ that we call the *commutator subgroup*. Again, if $G$ is abelian, then this commutator subgroup will simply be the identity. However, if $G$ is not abelian, then we can think of the commutator subgroup as measuring how far from being abelian it actually is. Thus, in general, we might say that more abelian the group is, the smaller its commutator subgroup, and the less abelian it is, the larger its commutator subgroup. For $S_3$, the commutator subgroup is the same as its single Sylow 3-subgroup, $\{ (1 \ 2 \ 3), (1 \ 3 \ 2) \}$. 
Recall now our earlier discussion of Sylow p-subgroups where our theorem said that if \( p^n \) is the highest power of a prime \( p \) that divides into the order of our group \( G \), then \( G \) will have a subgroup of order \( p^n \), a Sylow p-subgroup. We’ll now state our second and third Sylow Theorems.

**The Second Sylow Theorem:** Let \( G \) be a finite group, and let \( p \) be a prime that divides the order of \( G \). Then all Sylow p-subgroups of \( G \) are conjugate to one another.

**The Third Sylow Theorem:** The number of Sylow p-subgroups of a finite group \( G \) is a divisor of the order of \( G \).

Hence, from this it follows that if our Sylow p-subgroup is not normal, then we can find all the Sylow p-subgroups just by taking conjugates of a single Sylow p-subgroup. If we go back to our multiplication table for \( S_3 \), we can easily verify that all the subgroups of order 2 are conjugate.
For example, we have three subgroups of order 2. Namely, \( \{ (1)(2)(3) \} \), \( \{ (1)(2)(3) \} \), and
\( \{ (1)(2)(3) \} \). If we now create some conjugates by multiplying \( \{ (1)(2)(3) \} \) by \( (1 \ 3) \) and \( (2 \ 3) \) [Note that each of these elements is its own inverse], then we obtain:
\[
(1 \ 3) \{ (1)(2)(3) \} (1 \ 3) = \{ (1)(2)(3) \} \quad \text{and} \quad (2 \ 3) \{ (1)(2)(3) \} (2 \ 3) = \{ (1)(2)(3) \} .
\]
Thus, the other two groups are conjugate to the first, and hence, they are all conjugate to each other.

The second concept we want to look at is that of a commutator. Basically, if \( x, y \in G \),
then the *commutator* of \( x \) and \( y \) is the product \( xyx^{-1}y^{-1} \). Notice that if \( G \) is an abelian group or if \( x \) and \( y \) commute with one another, then \( xyx^{-1}y^{-1} = xx^{-1}yy^{-1} = e \), the identity element in \( G \). On the other hand, if \( x \) and \( y \) don’t commute with one another, but if their corresponding permutations don’t have much in common, then their commutator probably won’t result in too many changes. For example, let’s suppose that
\[
X = (1 \ 2 \ 3)(4 \ 5 \ 6) \quad \text{and} \quad Y = (6 \ 7 \ 8)(9 \ 10) .
\]
Then \( X^{-1} = (6 \ 5 \ 4)(3 \ 2 \ 1) \) and \( Y^{-1} = (10 \ 9)(8 \ 7 \ 6) \). The only item both \( X \) and \( Y \) permute is 6, and their commutator is,
\[
XYX^{-1}Y^{-1} = (1 \ 2 \ 3)(4 \ 5 \ 6)(6 \ 7 \ 8)(9 \ 10)(6 \ 5 \ 4)(3 \ 2 \ 1)(10 \ 9)(8 \ 7 \ 6) = (5 \ 6 \ 8)
\]
Thus, even though our permutations don’t commute, the commutator still undoes quite a bit of what gets moved around.

Now let’s suppose that we take all the commutators in our group and form all possible, finite products with them. This will generate a subgroup of $G$ that we call the *commutator subgroup*. Again, if $G$ is abelian, then this commutator subgroup will simply be the identity. However, if $G$ is not abelian, then we can think of the commutator subgroup as measuring how far from being abelian it actually is. Thus, in general, we might say that more abelian the group is, the smaller its commutator subgroup, and the less abelian it is, the larger its commutator subgroup. For $S_3$, the commutator subgroup is the same as its single Sylow 3-subgroup, $\left\{ \begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix} \right\}$. 
1. Find the conjugate of $(1 \ 2 \ 3)$ by $(1 \ 7)$.

2. Find the commutator of $(1 \ 2 \ 3)$ by $(1 \ 7)$.

3. **Prove:** If $G$ is a group (not necessarily finite), $H$ is a subgroup of $G$, and $a \in G$, then $aH a^{-1}$ is also a subgroup of $G$.

4. **Prove:** If $G$ is a group (not necessarily finite), $a \in G$, and $x \in G$ such that the order of $\langle x \rangle$ in $G$ is $\| \langle x \rangle \| = n$, then the order of the conjugate of $x$, $ax a^{-1}$, is also $n$.

5. **Prove:** If $G$ is a group (not necessarily finite), and $a,b \in G$, then $aba^{-1} = e$ if and only if $b = e$.
1. Find the conjugate of \((1\ 2\ 3)\) by \((1\ 7)\).

\[(1\ 7)(1\ 2\ 3)(1\ 7) = (7\ 2\ 3)\]

2. Find the commutator of \((1\ 2\ 3)\) by \((1\ 7)\).

\[(1\ 7)(1\ 2\ 3)(1\ 7)(3\ 2\ 1) = (7\ 2\ 3)(3\ 2\ 1) = (1\ 3\ 7)\]

3. **Prove:** If \(G\) is a group (not necessarily finite), \(H\) is a subgroup of \(G\), and \(a \in G\), then \(aHa^{-1}\) is also a subgroup of \(G\).

**Proof:** In order to show that \(aHa^{-1}\) is a subgroup of \(G\), we need to establish both closure and the existence of inverses. Thus, suppose that \(b, c \in aHa^{-1}\). Then there exist \(x\) and \(y\) in \(H\) such that \(b = axa^{-1}\) and \(c = aya^{-1}\). Hence, \(bc = (axa^{-1})(aya^{-1}) = a(xy)a^{-1} \in aHa^{-1}\) since \(xy \in H\). Now suppose that \(x \in H\). Then it is also the case that \(x^{-1} \in H\). Hence, \(axa^{-1}\) and \(ax^{-1}a^{-1}\) are both elements of \(aHa^{-1}\). Furthermore, \((axa^{-1})(ax^{-1}a^{-1}) = ax(aa^{-1})x^{-1}a^{-1} = a(xx^{-1})a^{-1} = aa^{-1} = e\). Therefore, inverses exist in \(aHa^{-1}\), and \(aHa^{-1}\) is a subgroup of \(G\). \(\square\)

4. **Prove:** If \(G\) is a group (not necessarily finite), \(a \in G\), and \(x \in G\) such that the order of \(\langle x \rangle\) in \(G\) is \(|\langle x \rangle| = n\), then the order of the conjugate of \(x\), \(axa^{-1}\), is also \(n\).

**Proof:** Let \(G\) be a group, \(a \in G\), and \(x \in G\) such that the order of \(\langle x \rangle\) in \(G\) is \(|\langle x \rangle| = n\), and consider the order of \(axa^{-1}\). If we raise this element to \(n^{th}\) power, then we obtain \((axa^{-1})^n = axa^{-1} \cdot axa^{-1} \cdot axa^{-1} \cdot \cdots \cdot axa^{-1} = axa^{-1} = axa^{-1} = e\). Additionally, if there were a natural number \(m < n\) such that \((axa^{-1})^m = e\), then this would imply that \(x^m = [a^{-1}(axa^{-1})a]^m = a^{-1}(axa^{-1})^m a = a^{-1} a = e\) which contradicts our assumption that \(|\langle x \rangle| = n\). Therefore, the order of the conjugate of \(x\), \(axa^{-1}\), is also \(n\). \(\square\)

5. **Prove:** If \(G\) is a group (not necessarily finite), and \(a, b \in G\), then \(aba^{-1} = e\) if and only if \(b = e\).

**Proof:** Suppose \(G\) is a group and \(a, b \in G\). Since our claim involves “if and only if,” we’ll have to prove the implication in both directions.
($\Rightarrow$) Suppose $aba^{-1} = e$. Then $a^{-1}(aba^{-1})a = a^{-1}ea \Rightarrow ebe = a^{-1}a \Rightarrow b = e$.

($\Leftarrow$) Suppose $b = e$. Then $aba^{-1} = aea^{-1} = aa^{-1} = e$.

Therefore, $aba^{-1} = e$ if and only if $b = e$. □
Many people have either written or talked about how the cube can mostly be solved using either conjugates or commutators, and so let’s look at a few ways in which we are already using them. First, at the very beginning when I am trying to correctly place the corners on the top face of the cube, I often do the move $R^{-1}DR$ which is a conjugate. Thus, let’s think about what this move does for us. My goal with this move is to place something in the up-front-right ($UFR$) corner. To do this, I position the cubelet that I want to move there in the down-front-left ($DFL$) corner. Then I do $R^{-1}$. That moves the up-front-right ($UFR$) corner to the down-front-right ($DFR$) position. Next, I do $D$, and this moves my cubelet from $DFL$ to $DFR$. And finally, I do $R$, and that rotates my cublet from the down-front-right ($DFR$) position back into the up-front-right ($UFR$) corner that was my goal. In a nutshell, you can say that we shifted things from the top face to a workspace down below, moved something into the workspace, and then moved it back to the top row.

$R^{-1}DR$
When we do a commutator on Rubik’s cube, the idea is that we are, most of the time, partially undoing what we have previously done. In particular, what happens when we do a commutator like $R^{-1}D^{-1}RD$ on the cube is that some of the cubelets get move around, but others stay right where they are, and anytime we move just a few cubelets, that gives us a tool we can use for easily solving the cube. Thus, let’s examine this particular commutator, $R^{-1}D^{-1}RD$, in greater detail. It, by the way, is the move that we usually use at the end to get our final corner cubelets turned correctly. If we do this move just once, then we’ll transpose two sets of corner cubelets, and we’ll cycle three edge cubelets,

$$(DB \ DR \ FR)(DRF \ UFR)(DBR \ DLB).$$

Thus, if we repeat this operation a second time, then we’ll restore the corner cubelets and just cycle the edge cubelets. However, when I do this, my corner cubelets, while being in the right corners, have also been twisted clockwise through an angle of $120^\circ$. And as you might suspect from the presence of 3 & 2-cycles that we have above for $R^{-1}D^{-1}RD$, repeating this move 6 times, the least common multiple of 2 and 3, will finally restore everything back to its starting point. And now you can see why this is our finishing move for the cube. At the end, we have all the cubelets in their correct positions, but some of the corner cubelets on top are usually twisted. To untwist them, we apply the algorithm $(R^{-1}D^{-1}RD)^2$ until we get one corner untwisted. Then we rotate the top to move another twisted corner into position, and we repeat with $(R^{-1}D^{-1}RD)^2$ until that one is untwisted. However, the one thing that we are mathematically guaranteed is that the number of times we have to do $(R^{-1}D^{-1}RD)^2$ is always going to be some multiple of 3. Thus,
suppose we have to do $(R^{-1}D^{-1}RD)^2$ just three times. Then
$[(R^{-1}D^{-1}RD)^2]^3 = (R^{-1}D^{-1}RD)^6 = e$. In other words, since our algorithm has order 6, by the
time we are done untwisting the cubelets, everything has been returned to its proper
position and orientation.

$(R^{-1}D^{-1}RD)^2, (R^{-1}D^{-1}RD)^4, (R^{-1}D^{-1}RD)^6$
Many people find group theory pretty difficult because the logic behind it seems algebraic to the extreme and geometric not at all. However, there are a few ways to visualize groups that we’ll now discuss. The first way is by constructing what we call a Cayley graph. To do this, we usually start with a minimal set of generators for the group, and then we create the different elements by multiplying them together. We connect our elements by lines that are colored differently to represent the different generators, and when we are done, the result is a wonderful, symmetrical diagram. Below is a Cayley diagram for $D_3$ where I’ve used blue for the rotation and red for the flip. I’ve also labeled a few lines so that you can easily see the relation that we discovered earlier that $FR = RRF$. 

\[ R^2 F = RRF = FR \]
Now let me give a few more details on how to construct such a diagram. First, let’s start with the multiplication table for $D_3$.

<table>
<thead>
<tr>
<th></th>
<th>$e$</th>
<th>$R$</th>
<th>$R^2$</th>
<th>$F$</th>
<th>$FR$</th>
<th>$FR^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e$</td>
<td>$e$</td>
<td>$R$</td>
<td>$R^2$</td>
<td>$F$</td>
<td>$FR$</td>
<td>$FR^2$</td>
</tr>
<tr>
<td>$R$</td>
<td>$R$</td>
<td>$R^2$</td>
<td>$e$</td>
<td>$FR^2$</td>
<td>$F$</td>
<td>$FR$</td>
</tr>
<tr>
<td>$R^2$</td>
<td>$R^2$</td>
<td>$e$</td>
<td>$R$</td>
<td>$FR$</td>
<td>$FR^2$</td>
<td>$F$</td>
</tr>
<tr>
<td>$F$</td>
<td>$F$</td>
<td>$FR$</td>
<td>$FR^2$</td>
<td>$e$</td>
<td>$R$</td>
<td>$R^2$</td>
</tr>
<tr>
<td>$FR$</td>
<td>$FR$</td>
<td>$FR^2$</td>
<td>$F$</td>
<td>$R^2$</td>
<td>$e$</td>
<td>$R$</td>
</tr>
<tr>
<td>$FR^2$</td>
<td>$FR^2$</td>
<td>$F$</td>
<td>$FR$</td>
<td>$R$</td>
<td>$R^2$</td>
<td>$e$</td>
</tr>
</tbody>
</table>

We’ll begin our diagram with one dot for $e$, and then emerging from this dot we’ll draw a blue arrow for $R$ that we’ll let terminate at a dot with the same name. Next, we construct another blue arrow emanating from the dot labeled $R$, and we let this arrow terminate at a dot that we’ll label $R^2$. If we repeat this process one more time, then that will take us back to $e$ since $R^3 = e$. We now begin again at $e$ with a red arrow for $F$ that, again, we’ll terminate at a dot with the same name. Also, since $F$ has order 2, it’s customary not to put an arrow head on this one. At this point, there are just two elements left in our multiplication table that are not yet in our diagram, $FR$ and $FR^2$. Hence, construct a blue line emerging from the dot labeled $F$, and let it terminate at a dot that we’ll label $FR$. And as before, add a blue arrow to $FR$, and let it terminate at $FR^2$. And then as you would expect, a blue arrow emanating from $FR^2$ will take us back to $F$ since $FR^3 = F$.

At this point, your connected dots and arrows should look like the diagram below.
And now there is just one thing missing. Since our group is generated by the elements $R$ and $F$, every dot in our Cayley graph needs both a red arrow and a blue arrow emanating from it to show us where the multiplication takes us. However, since we know that all the elements in our group are now represented by dots in the diagram, all we need to do is to look at our multiplication table above to see where the red arrows will take us if we follow each of $FR$ and $FR^2$ by $F$. And below is our completed Cayley graph!
The second diagram I want to show you is called a cycle graph, and I really like it better. Basically, for every element in your group, you make a sketch that shows the cycle it creates. I like this because I think one of the most important things to realize about group theory is that all the complex structures we might create are created by simply combing cycles in various ways. Also, if we have something like a cycle of length 4 in our graph, then that’s clearly going to contain a cycle of length 2. In this case, we don’t make a separate diagram for the 2-cycle. We just recognize that it’s already part of the 4-cycle. Below now is a cycle graph for $D_3$. Recall that it has one cyclic subgroup of order 3 and three separate cyclic subgroups of order 2. Also, the blue dot in the middle represents the identity element in the group. Think of it as your starting point!
As with the Cayley graphs, let’s give a little more detail on how to do the construction using the multiplication table for $D_3$ that we presented earlier. Again we start with one dot for $e$. We now go to the element $R$ in our table and note that it has order 3. This is going to result in a cycle of length 3 in our cycle graph. Additionally, since $R^2$ is part of this cycle, we can now skip in our table to $F$. Since the order of $F$ is 2, we draw a visual representation of a 2-cycle that starts at $e$. Similarly, both $FR$ and $FR^2$ have order 2, and so we add two more 2-cycles to our diagram. And now we’re done because all the elements of our group are now present in our cycle graph! Below is the final product with the elements labeled.

![Cayley graph diagram](image)

Both Cayley graphs and cycle graphs can help us to better understand the structure of a group just so long as its not too large. When we get into larger groups, though, these diagrams get very complicated! Also, one problem with cycle graphs is that once we get to groups of order 16, we can actually have different, non-isomorphic groups that
generate the same cycles. Nonetheless, as long as we stay below order 16, each group will have a unique cycle graph. Furthermore, even for larger groups we can use a cycle graph to help show us what groups it’s not isomorphic to.

As a final note, for both cyclic and dihedral groups, the cycle graphs are always pretty simple. For example, the cycle graph for a cyclic group of order $n$ can be represented by a regular polygon with $n$ sides, and the dihedral group $D_n$ will have one cycle that can be represented by an $n$-sided polygon, and then it will also have $n$ additional cycles of order 2. Thus, the cycle graph for $D_4$ looks like the following (if I do a quick and dirty sketch in PowerPoint). Cycle graphs and Cayley graphs of several groups may be found in the program Group Explorer.
1. Draw a Cayley graph for $D_4$, the group of symmetries of the square.

2. Draw a Cayley graph for each of the abelian groups below of order 4.
   a. $\mathbb{Z}_4$
   b. $\mathbb{Z}_2 \oplus \mathbb{Z}_2$

3. Draw cycle graphs for each of the abelian groups below of order 4.
   a. $\mathbb{Z}_4$
   b. $\mathbb{Z}_2 \oplus \mathbb{Z}_2$

4. Draw cycle graphs for each of the abelian groups below of order 8.
   a. $\mathbb{Z}_8$
   b. $\mathbb{Z}_2 \oplus \mathbb{Z}_4$
   c. $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$
1. Draw a Cayley graph for $D_4$, the group of symmetries of the square.
2. Draw a Cayley graph for each of the abelian groups below of order 4.

a. $\mathbb{Z}_4$
b. $\mathbb{Z}_2 \oplus \mathbb{Z}_2$
3. Draw cycle graphs for each of the abelian groups below of order 4.

a. \( \mathbb{Z}_4 \)

\[
\begin{array}{c}
\text{e} \\
\text{a} \\
\text{a}^3 \\
\text{g} \\
\end{array}
\]

b. \( \mathbb{Z}_2 \oplus \mathbb{Z}_2 \)

\[
\begin{array}{c}
\text{h} \\
\text{h} \\
\text{e} \\
\text{i} \\
\text{i}
\end{array}
\]
4. Draw cycle graphs for each of the abelian groups below of order 8.

a. $\mathbb{Z}_8$
b. $\mathbb{Z}_2 \oplus \mathbb{Z}_4$
c. $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. 
GROUPS OF SMALL ORDER

In this chapter I just want to do a quick survey of groups of small order. Namely, groups that have orders 1 through 12 plus $S_4$ which has order 24. Additionally, don’t forget that, among other things, $S_4$ represents the 24 different positions we put a cube in by rotating the whole cube clockwise about the up face, right face, or front face. Remember, also, that we are going to call the group generated by these moves Benton’s Group. Benton’s Group, Benton’s Group, Benton’s Group! Make me famous!!! 😎 Also, for more information on all of these groups, look up the list of small groups, http://en.wikipedia.org/wiki/List_of_small_groups, in the Wikipedia, or download the free software program Group Explorer by Nathan Carter, http://groupexplorer.sourceforge.net/. Below, for each order we will list the possible groups up to isomorphism. That essentially means that if two groups are isomorphic, we’re pretty much going to call them the same group even if the elements are described differently or if they arise from different contexts. Furthermore, keep in mind that if a group has prime order, then it has to be cyclic since the only subgroups it can have are itself and the identity. If it had any other type of subgroup, then the order of that subgroup would divide the prime which is impossible. Thus, every non-identity element of a cyclic group of prime order generates that group. Also keep in mind that if a group is abelian, then all of its subgroups will automatically be normal subgroups.
Groups of order 1:

There is only one group of order 1, and that’s the identity group, the trivial group. Below is its puny little multiplication table. Also, it’s abelian.

\[
\begin{array}{c|c}
  e & e \\
  \hline
  e & e \\
\end{array}
\]

Groups of order 2:

Since 2 is a prime number, the only group of order 2 is the cyclic group \( \mathbb{Z}_2 \), and it’s abelian.

Groups of order 3:

Since 3 is a prime number, the only group of order 3 is the cyclic group \( \mathbb{Z}_3 \), and it’s abelian.

Groups of order 4:

There are two groups of order 4 and both are abelian. Thus, from the Fundamental Theorem of Finite Abelian Groups, we know exactly what they are. One must be the
cyclic group \(\mathbb{Z}_4\), and the other is the direct sum of two cyclic groups, \(\mathbb{Z}_2 \oplus \mathbb{Z}_2\) (also frequently written as the direct product \(\mathbb{Z}_2 \times \mathbb{Z}_2\)). This latter group, by the way, is also called the *Klein four-group* after Felix Klein (1849 – 1925). It is the first group we encounter which is not cyclic.

**Groups of order 5:**

Since 5 is a prime number, the only group of order 5 is the cyclic group \(\mathbb{Z}_5\), and it’s abelian.

**Groups of order 6:**

There are two groups of order 6, one is abelian and the other is nonabelian, and this is also the first time we encounter a nonabelian group in our list. The abelian group is the cyclic group \(\mathbb{Z}_6\). You would think that we would also invoke the Fundamental Theorem of Finite Groups and list \(\mathbb{Z}_2 \oplus \mathbb{Z}_3\), but it turns out that this group is isomorphic to \(\mathbb{Z}_6\) and so we don’t need to engage in a needless repetition, \(\mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3\).

The nonabelian group of order 6 is \(S_3\), the group of the six permutations that we can make of three objects, and it is isomorphic to \(D_3\), the dihedral group that describes the symmetries of an equilateral triangle (\(S_3 \cong D_3\)).
Groups of order 7:

Since 7 is a prime number, the only group of order 7 is the cyclic group $\mathbb{Z}_7$, and it’s abelian.

Groups of order 8:

There are several groups of order 8, three are abelian and two are nonabelian. As usual, it’s not too hard to identify the abelian groups, thanks to the Fundamental Theorem of Finite Abelian Groups. We’ve got the cyclic group of order 8 ($\mathbb{Z}_8$), $\mathbb{Z}_2 \oplus \mathbb{Z}_4$, and $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. As for the two nonabelian groups, we should be able to immediately guess that one of them will be the dihedral group of the symmetries of a square, $D_4$. The last nonabelian group of order 8, however, is going to be something completely new to us. It’s called the quaternion group, and its multiplication table is given below.

\[
\begin{array}{cccccccc}
1 & -1 & i & -i & j & -j & k & -k \\
1 & 1 & -1 & i & -i & j & -j & k & -k \\
-1 & -1 & 1 & -i & i & -j & j & -k & k \\
i & i & -i & 1 & k & -k & j & -j & k \\
i & -i & i & -i & 1 & k & -k & j & -j \\
j & j & -j & -k & k & -1 & 1 & i & -i \\
j & -j & j & k & -k & 1 & -1 & -i & i \\
k & k & -k & j & -j & -i & i & -1 & 1 \\
k & -k & k & -j & j & i & -i & 1 & -1
\end{array}
\]
As you might notice from the multiplication table, quaternions are in some ways like an extension of complex numbers, and in other ways they are like vectors. They were discovered by the mathematician William Rowan Hamilton (1805 – 1865), and they have a history of applications in both math and physics. However, in more recent times they have become an essential part of the mathematics behind the 3D animation that so many people enjoy today. Mathematically, the quaternion group is the first group we encounter in which all the subgroups are normal, but the group itself is nonabelian.

Groups of order 9:

There are two groups of order 9, and they are both abelian. They are the cyclic group $\mathbb{Z}_9$ and direct sum $\mathbb{Z}_3 \oplus \mathbb{Z}_3$.

Groups of order 10:

There are two groups of order 10, and one is abelian and the other nonabelian. One is the cyclic group $\mathbb{Z}_{10} = \mathbb{Z}_2 \oplus \mathbb{Z}_5$, and the other is the dihedral group $D_5$. 
Groups of order 12:

There are two abelian groups of order 12 and three nonabelian groups, but the only one we will be interested in is the nonabelian dihedral group $D_6$. This is because our two-squares group, $\langle R^2, U^2 \rangle$, is isomorphic to $D_6$. This dihedral group has 16 subgroups, the identity, the whole group, seven subgroups of order 2, one subgroup of order 3, three subgroups of order 4, and three subgroups of order 6.

Groups of order 24:

There are three groups of order 24 with one being abelian and the other two nonabelian. The abelian group is $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$, and the nonabelian groups are $S_4 \times \mathbb{Z}_4$ and $S_4$. Of course, the only one we are interested in is $S_4$, the group of all permutations of four objects which is the group we obtain by looking at rotations of the entire cube, i.e. what I like to call Benton’s Group\(^1\). This group has thirty different subgroups. Make me famous!

\(^1\) Make me famous!
Previously, we talked about what it means for two groups to be isomorphic, and we explained that this means that they have the same structure and essentially are identical except for whatever labels are used to describe the elements. We now want to look at a slightly more general concept, that of two groups being homomorphic. The word homomorphic means “same shape,” and so let’s discuss what we mean when we say that two groups, $G_1$ and $G_2$, have the same shape. If we are going to say that these two groups have the same shape, then we need some sort of connection between them, and, of course, the way in which we connect two sets in mathematics is with a function. Thus, let’s assume that we have a function from $G_1$ onto $G_2$, $f: G_1 \rightarrow G_2$. Recall that the word “onto” in math simply means that $G_2$ is the entire range of our function. Thus, for any $y \in G_2$, there exists an $x \in G_1$ such that $f(x) = y$. At this point, let’s reminds ourselves that groups are not merely sets, they are sets with binary operations defined on them. That is, in each set we have a way of combining two elements to get a third element. And now, using the multiplication defined within each group, we can explain what we mean when we say that the two groups have the same shape. By this we mean that not only do we have a function $f$ from $G_1$ onto $G_2$, but it is also the case that if in $G_1$ we have that $ab = c$, then in $G_2$ we will have that $f(a)f(b) = f(c)$. This means that multiplication in one group will correspond to multiplication in the other group. Also, another way to write this last equation is as $f(a)f(b) = f(ab)$ or $f(ab) = f(a)f(b)$, and any function $f$ from $G_1$ onto $G_2$ with this kind of property is what we call a homomorphism.
There are several easy theorems to prove about homomorphisms, and I’ll start with one that shows that a homomorphism takes the identity element in one group to the identity element in the other group.

**Theorem:** Let $f: G_1 \to G_2$ be a homomorphism from $G_1$ onto $G_2$, and suppose $e_1$ is the identity element in $G_1$ and $e_2$ is the identity element in $G_2$. Then $f(e_1) = e_2$.

**Proof:** Let $a \in G_1$. Then $a = ae_1$. Hence, $f(a) = f(ae_1) = f(a)f(e_1)$. From this we can conclude that $f(a)^{-1}f(a) = f(a)^{-1}f(a)f(e_1) \Rightarrow e_2 = e_2f(e_1) \Rightarrow e_2 = f(e_1)$. □

Another fact that is easy to prove about homomorphisms is that they take the inverse in one group to the inverse in the other group. In other words, $f(a^{-1}) = f(a)^{-1}$. This is easy to prove, but for now we’ll just assume it’s true so that we can get on with showing you why normal subgroups are so important and, also, what they have to do with homomorphisms. We’ll begin with the following definition.

**Definition:** If $f: G_1 \to G_2$ is a homomorphism from $G_1$ onto $G_2$, then the *kernel* of the homomorphism is the set of all elements that get sent to $e_2$ (the identity in $G_2$) by the homomorphism.

This next theorem is one that I’m going to prove just for finite groups even though it is actually true for all groups. I’ll let you extend the result to all groups as an exercise.
Theorem: Let $G_1$ and $G_2$ be finite groups, let $f : G_1 \to G_2$ be a homomorphism from $G_1$ onto $G_2$, and let $K = \{x \in G_1 \mid f(x) = e_2\}$. Then $K$ is a subgroup of $G_1$.

Proof: Since we are assuming that our groups are finite, to show that $K$ is a subgroup of $G_1$ requires us only to show that $K$ is closed under multiplication. Thus, suppose $x, y \in G_1$. Then $f(xy) = f(x)f(y) = e_2 e_2 = e_2$, the identity element in $G_2$. Therefore, $xy \in K$ and $K$ is a subgroup of $G_1$ since $K$ is closed under multiplication. □

Now that we know that the kernel of a homomorphism is a subgroup of our group, we’re next going to show that it is a normal subgroup. Recall that this means that for any $a \in G_1$, we have that $aKa^{-1} = K$. Also, at this point we’ll drop the requirement that our groups be finite as we’ll assume that you either have or soon will have taken time to extend the result of the previous theorem.

Theorem: Let $G_1$ and $G_2$ be groups, let $f : G_1 \to G_2$ be a homomorphism from $G_1$ onto $G_2$, and let $K = \{x \in G_1 \mid f(x) = e_2\}$. Then $K$ is a normal subgroup of $G_1$.

Proof: To prove this, it will suffice to show that if $a \in G_1$ and $x \in K$, then $axa^{-1} \in K$. However, this should be a very obvious fact to us at this point since $f(axa^{-1}) = f(a)f(x)f(a^{-1}) = f(a)f(x)f(a^{-1}) = f(a)e_2f(a)^{-1} = f(a)f(a)^{-1} = e_2$. Therefore, $axa^{-1} \in K$ and $K$ is a normal subgroup of $G_1$, $K \triangleleft G_1$. □
We may now begin to explain why normal subgroups are so important in group theory. They reason is because they have a very important connection with homomorphisms. In fact, it can be shown that not only is the kernel of a homomorphism a normal subgroup, but it is also the case that every normal subgroup gives rise to a homomorphism from one group onto another. Thus, if we know what the normal subgroups of a given group are, then we know what kinds of homomorphisms are possible with respect to that group.

Now let’s look at a few simple examples. Let’s denote the set of integers by $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ and the integers modulo 2 by $\mathbb{Z}_2 = \{0, 1\}$, and let’s define a homomorphism $f : \mathbb{Z} \to \mathbb{Z}_2$ by

$$f(x) = \begin{cases} 0 & \text{if } x \text{ is even} \\ 1 & \text{if } x \text{ is odd} \end{cases}.$$  

Then, given that this is a homomorphism, its kernel is the set of all even integers, and we know that this kernel is both a subgroup and a normal subgroup of $\mathbb{Z}$. (Actually, we get normality for free in this case because $\mathbb{Z}$ is abelian, and that means that all of its subgroups are normal.)

Notice that in our new group $\mathbb{Z}_2 = \{0, 1\}$, all the particular information about our integers has been lost except for whether the integer is even or odd. In other words, if I tell you that $f(x) = 0$, then all you know about $x$ is that it’s some even integer. In mathematics,
we often like to write the set of even integers as $2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$, and the group that our homomorphism has given back to us we write as $\mathbb{Z}/2\mathbb{Z}$. This last expression looks like division, and that’s exactly how we want to think about it, only in this case, we are saying that we are taking the integers and we are dividing out the differences between the even integers. That means that we’re creating a new structure in which all even integers appear the same and all odd integers appear the same. In this instance, in the new structure we have two cosets, one consisting of the even integers and one consisting of the odd integers, and we can add them by simply saying that $even + even = even$, and $odd + even = odd$. This results in a group that is isomorphic to the integers modulo 2, $\mathbb{Z}_2$. This new structure is called a quotient structure or a quotient group, and if you take a formal course on abstract algebra, then you’ll spend a lot of time on these things. However, in this work I only want to give you an introduction to the basic idea, and no more! Thus, here are the big ideas:

1. Every normal subgroup $N$ of a group $G$ gives rise to a homomorphism.
2. This homomorphism also results in a quotient structure or quotient group that we write as $G/N$.
3. In this quotient structure $G/N$, all the elements of the subgroup $N$ appear as identical or indistinguishable from one another.
4. If we start with an onto homomorphism $f : G \to H$, then $K$, the kernel of $f$, is a normal subgroup of $G$.

5. The structure of $G / K$ is identical to the structure of $H$. In other words, $G / K$ is isomorphic to $H$, $G / K \cong H$.

Well, this is taking us deeper into the depths of abstract algebra than we need to go at this point, but, nonetheless, I do want to show you one particular homomorphism that can lead to some interesting results regarding Rubik’s cube. In particular, let’s fix $a \in G$ and let’s suppose that $x \in G$ is just any element in $G$. Then we can define a homomorphism $f_a : G \to G$ by $f_a(x) = axa^{-1}$. We claim that this function is not only a homomorphism, but it’s also a one-to-one homomorphism. That means it’s an isomorphism. Furthermore, whenever we have an isomorphism from a group $G$ back onto itself, we call it an automorphism.

In the next chapter, we will use automorphisms to help us discover new patterns that we can make on the surface of Rubik’s cube. For example, suppose we have a sequence of moves that we’ll just call $Y$ that happens to produce a pleasing pattern. Now let’s suppose that we have another sequence of moves that we’ll call $X$. Then $f_X$ defines an automorphism from the Rubik’s cube group to the Rubik’s cube group, and if we’re lucky, then $XYX^{-1}$ will transform the pattern $Y$ into another pleasing pattern.

And now, let’s close by showing that $f_a : G \to G$ defined by $f_a(x) = axa^{-1}$ is an automorphism.
Theorem: Let $G$ be a group, fix $a \in G$, and define $f_a : G \to G$ by $f_a(x) = axa^{-1}$. Then $f_a : G \to G$ is an automorphism.

Proof: We’ll first show that $f_a : G \to G$ is one-to-one. Thus, suppose that $x, y \in G$ and that $f_a(x) = f_a(y)$. Then $f_a(x) = f_a(y) \Rightarrow axa^{-1} = aya^{-1} \Rightarrow a^{-1}(axa^{-1})a = a^{-1}(aya^{-1})a \Rightarrow x = y$.

Hence, $f_a : G \to G$ is one-to-one. Now let’s consider $f_a(xy)$. By definition, $f_a(xy) = a(xy)a^{-1} = ax(ax^{-1})ya^{-1} = (axa^{-1})(aya^{-1}) = f_a(x)f_a(y)$. Therefore, $f_a : G \to G$ is a homomorphism, and it now follows that $f_a : G \to G$ is an automorphism.

And as a final note, this particular type of automorphism is so special in group theory that we give it a particular name. We call it an inner automorphism.
1. **Prove:** If $f : G \to H$ is a homomorphism and $a \in G$, then $f(a^{-1}) = f(a)^{-1}$.

2. **Prove:** Let $G_1$ and $G_2$ be groups (not necessarily finite), let $f : G_1 \to G_2$ be a homomorphism from $G_1$ onto $G_2$, and let $K = \{ x \in G_1 \mid f(x) = e_2 \}$. Then $K$ is a subgroup of $G_1$. 
1. **Prove:** If \( f : G \to H \) is a homomorphism and \( a \in G \), then \( f(a^{-1}) = f(a)^{-1} \).

**Proof:** Let \( G \) and \( H \) be groups, \( a \in G \), and let \( f : G \to H \) be a homomorphism. Then 
\[ e = f(a) \cdot f(a)^{-1} \quad \text{and} \quad e = f(e) = f(aa^{-1}) = f(a)f(a^{-1}) . \]
Therefore, since elements in groups have unique inverses, it follows that \( f(a^{-1}) = f(a)^{-1} \). \( \square \)

2. **Prove:** Let \( G_1 \) and \( G_2 \) be groups (not necessarily finite), let \( f : G_1 \to G_2 \) be a homomorphism from \( G_1 \) onto \( G_2 \), and let \( K = \{ x \in G_1 \mid f(x) = e_2 \} \). Then \( K \) is a subgroup of \( G_1 \).

**Proof:** In order to show that \( K \) is a subgroup of \( G_1 \), we need to establish both closure and the existence of inverses. Thus, suppose \( x, y \in G_1 \). Then 
\[ f(xy) = f(x)f(y) = e_2e_2 = e_2, \]
the identity element in \( G_2 \). Therefore, \( xy \in K \) and \( K \) is closed under multiplication. Now suppose \( x \in G_1 \) and consider \( x^{-1} \in G_1 \). Clearly, 
\[ e_2 = f(e_1) = f(xx^{-1}) = f(x)f(x^{-1}) = e_1 \cdot f(x^{-1}) = f(x^{-1}) . \]
Therefore, \( x^{-1} \in K \), and \( K \) is a subgroup of \( G_1 \). \( \square \)
We now just want to examine a few interesting patterns you can create on the surface of Rubik’s cube. However, our interest goes beyond just art. There are certainly many places where one can go and instantly find algorithms for all sorts of patterns for the cube, but we want to do more than that. As usual, we want to explain some of the math that comes with these patterns.

1. This first pattern is one of my favorites. In this case, the algorithm simply switches two front edge cubes with the corresponding back edge cubes. It’s simple, but elegant. Also, this algorithm generates a cyclic group of order 2, and that means that the algorithm is its own inverse.

\[(R^2 U^2)^3\]
2. This next pattern is created using elements of the slice group. Recall that the slice group effectively moves only the center slices of the cube, and thus, the corner cubes stay fixed. Consequently, a lot of nice patterns can be created using only slices. In the pattern below we have 6 dots centered on backgrounds of different colors. Notice that this element of the slice group has order 3.

\[ UD^{-1}RL^{-1}FB^{-1}UD^{-1} \]
3. This next pattern of six checkerboards comes from the slice squared group. Also, recall that this group is abelian.

\[ U^2 D^2 R^2 L^2 F^2 B^2 \]
4. In this pattern, we’ve taken the previous pattern and created a conjugate of the form $xyx^{-1}$. Recall, too, that multiplying all elements of the group in such a manner produces an inner automorphism of the group, and with luck, this will also transform one interesting pattern into another. In this case, we see our previous pattern of six checkerboards transformed into one of four checkerboards.

\[
\left( R^2U^2 \right)^3 U^2 D^2 R^2 L^2 F^2 B^2 \left( R^2U^2 \right)^3
\]
5. The next four pictures are going to be based on patterns from the slice squared group. We’ll first look at a pattern from this group, and then we’ll form a conjugate of that pattern using \( (R^2U^2)^3 \).
6. This time we’ll start with \( R^2 L^2 F^2 B^2 \) and then, again, form a conjugate with \( (R^2 U^2)^3 \).

\[
(R^2 U^2)^3 \, R^2 L^2 F^2 B^2 \, (R^2 U^2)^3
\]

\[
R^2 L^2 F^2 B^2
\]
7. This one is one of my favorites. It creates a center dot on two of the faces, a checkerboard on two, and stripes on the remaining two.

\[(R^2U^2)^3 R^2L^2F^2B^2(L^2U^2)^3\]
8. If you start with the red face in front and the white face to the right, then this will create 4 crosses with one of them a red Templar cross on a white background. I like this one because a few of my ancestors on my dad’s side were Knights Templar.

\[LUFLULDUDU^{-1}F^{-1}U^{-1}F^{-1}D^{-1}F^{-1}L^{-1}D^{-1}F^{-1}\]
9. Again start with the red face in front and the white fact to the right. This algorithm will produce 6 crosses with one of them a red Templar cross on a white background.

\[ L^2 R^{-1} F D^2 L^{-1} F^{-1} R L^{-1} F B^{-1} L F U^2 L^{-1} F^2 B \]
10. One thing I like to do is to see what new patterns I can create by combining

\[ UD^{-1}RL^{-1}FB^{-1}UD^{-1} \text{ with } \left(R^2U^2\right)^3. \] See what interesting things you can come up with!

Start with \( UD^{-1}RL^{-1}FB^{-1}UD^{-1} \), rotate the whole cube, and do \( UD^{-1}RL^{-1}FB^{-1}UD^{-1} \) again to get a pattern of four dots.

Take the 4-dot pattern and add \( \left(R^2U^2\right)^3 \), rotate the whole cube, and do \( \left(R^2U^2\right)^3 \) again. You should now have a 4-dot pattern combined with a checkerboard pattern!
11. And finally, this algorithm creates an incredible pattern called the superflip. Basically, every cubelet is in its home position, but every single edge cubelet has been flipped. It’s pretty easy to see that the group generated by this move has order 2, but what is not so obvious is that this element of the Rubik’s cube group commutes with every other element of that group. In fact, the only other element in the group that does that is the identity. In group theory, the set of all elements of a group that commute with every other element is called the center of the group, and the center of the Rubik’s cube group consists of only the identity and the superflip.

\[ UR^2FBRB^2RU^2LB^2RU^{-1}D^{-1}R^2FR^{-1}LB^2U^2F^2 \]

or

\[ FLULB^{-1}U^{-1}D^{-1}LF^{-1}U^{-1}B^{-1}RL^{-1}BF^2U^{-1}D^{-1}F^2B^2R^2U^{-1}D^{-1} \]
Now that we know a lot about the mathematics behind Rubik’s cube, it’s time to take a closer at the solution we use. The first part, of course, is pretty easy. When I’m trying to solve Rubik’s cube, I always begin with the green center cubelet on top so that I can finish the green face first. I begin with the goal of initially completing the green cross on top, and that is really very easy. I simply rotate faces until I get the green facelet of an edge cube positioned on the down face of the cube. I then rotate the down face until the other color on the edge cube matches the center cube. And finally, I rotate the appropriate face 180° to bring the green facelet to the up face. I then repeat until I’ve finished my green cross, and I don’t really have to formalize the procedure too much since I’m not that worried, yet, about what’s going on with the rest of the cube.

Once I’ve completed the green cross on the up face, I still improvise quite a bit to get the corners positioned. However, I do usually make use of the maneuvers $R^1DR$ and $FD^{-1}F^{-1}$ in order to get my corner cubelet placed with the right orientation. Sometimes,
though, the green facelet of a corner cubelet is on the down face of the cube, and when this happens I may do something like $DFD^{-1}F^{-1}R^{-1}D^{-1}R$ to rotate it in the bottom layer.

Once the green face is completed, I turn the cube over so that green is on the down face, and then I proceed in a systematic way to place the edge cubes in the middle layer. The two algorithms that are used in our solution are $URU^{-1}R^{-1}U^{-1}F^{-1}UF$ and $U^{-1}F^{-1}UFURU^{-1}R^{-1}$. What should be clear at this point is that both algorithms are products of commutators which means that they belong to the commutator subgroup of the Rubik’s cube group. Also, as we have seen previously, commutators have a tendency to move only a few elements. Given that, let’s look at the first algorithm in a bit more detail. If we perform only the first part, $URU^{-1}R^{-1}$, then the resulting permutation given as a product of cycles can be written as $(UB\; UR\; FR)(DRF\; UR)(UBL\; URB)$. We can now see the promise of this permutation. It contains a 3-cycle that involves two edge cubelets on the up face and the edge cubelet in the front-right position. Just what we want! It also involves a couple of 2-cycles that move corner cubelets, and one of them only switches corner cubelets on the up face. Unfortunately, the other one switches the up-front-right corner cubelet with the down-right-front corner cubelet, and that will mess
up the green face that we just completed. However, if we perform our algorithm twice, \((URU^{-1}R^{-1})^2\), then the result is just the 3-cycle \((FR \ UR \ UB)\), and that looks promising except for the fact that this also twists the down-right-front corner cublet into a different orientation. Thus, let’s see how the permutation \(U^{-1}F^{-1}UF\) might fix things for us. If we do this algorithm, then the resulting cycle structure is \((UL \ UF \ FR)(DRF \ UFR)(ULF \ UBL)\). What we immediately see is that our algorithm will once again permute two edge cubelets in the up face with the front-right edge cubelet and it will also switch the down-right-front corner cubelet with the up-front-right corner cubelet. Exactly what we need! Furthermore, when we multiply the two permutations together we get:

\[
(UB \ UR \ FR)(DRF \ UFR)(UBL \ URB)(UL \ UF \ FR)(DRF \ UFR)(ULF \ UBL)
\]

\[
=(UB \ UR \ UL \ UF \ FR)(UBL \ URB \ ULF).
\]

From this result we can see that the up-front edge cubelet moves into the front-right position, and everything else that happens is basically a permutation of cubelets on the up face. Absolutely perfect! Furthermore, when we try it out, we see that the facelet on the front of the up-front edge cubelet remains on the front face when it is moved to the front-right position. This means that our algorithm will work fine just so long as the cubelet that we want to move to the middle layer has the right facelet on the front face, but if its orientation is flipped, then that’s why we need our second algorithm, \(U^{-1}F^{-1}UFURU^{-1}R^{-1}\). If we look at the cycle structure for this one, then we get \((UL \ UF \ UB \ UR \ FR)(ULF \ URB \ UBL)\). For this one, we need to first get the cubelet we want to place moved into the up-right position, and then our algorithm will move it to the front-right position with the proper orientation.
Well, this argument may be a little hard to follow, and consequently, I recommend going through these algorithms yourself using the Rubik software mentioned at the start of this book so that you can follow exactly what happens with each little movement.

The next step in our solution to Rubik’s cube is to get the blue facelets on the up face for all of the edge cublets on our top layer, and we can achieve this with the help of the commutator \( R U R^{-1} U^{-1} \). However, when we look at the corresponding cycle structure, we see that this commutator moves an edge cubelet on the up face to the front-right position, \((FR \ UB)(DRF \ UFR)(UBL \ URB)\). Fortunately, there’s an easy fix for this. Simply begin by turning the front face clockwise \((F)\) before doing your commutator, and then turn it back again counterclockwise \((F^{-1})\) when you are done. In other words, do \(FRUR^{-1}U^{-1}F^{-1}\). This maneuver will constrain all the movement to the top face, \((UB \ UF \ UR)(ULF \ UFR)(UBL \ URB)\). When we perform this algorithm, we’ll also see that the up-left cubelet never moves, and that two of our edge cubelets get flipped as
we go from up-back to up-front and up-front to up-right. Consequently, often all we have
to do is to simply repeat this algorithm until all the edge cubelets have the proper facelet
on the up face, and if that doesn’t work, then you may have to throw in a rotation of the
up face in between applications of the algorithm. Something else to notice is that if we
perform this algorithm three times, then the resulting cycle structure is going to be
\((ULF \ UFR)(UBL \ URB)\). In other words, we switch the two front corner cubelets on
top with each other and we also switch the two back corner cubelets. Additionally, when
we actually perform this maneuver, we see that the corner cubelets also get rotated in the
process. This is a move that could be useful in creating an alternate solution to Rubik’s
cube.

Now that we have the edge facelets on the up face properly oriented, we just need to
permute the up face edge cubelets until they are all in their proper positions. The
algorithm we use for this is \(RUR^{-1}URU^{-2}R^{-1}\). Let’s break this down a bit. First, perform
this algorithm, and keep track of the up-front edge cubelet. What you should notice is that as you do $U$, $U^2$, and $U^3$, the up-front edge cubelet basically just winds up right back where it started. No change. However, notice also the presence of the conjugates $RUR^{-1}$ and $RU^2R^{-1}$ in our algorithm. Basically what we are doing with these conjugates is that we are moving an edge cubelet out of the up-right position, rotating the up face, and then moving our edge cubelet back into the up-right position, and the end result of $RUR^{-1}URU^2R^{-1}$ is that we permute three of the edge cubelets on the up face with one another. Also, fortunately, nothing below the top layer is disturbed once we complete our $RUR^{-1}URU^2R^{-1}$ algorithm, and the cycle structure for this algorithm is $(UL\ UR\ UB)(UBL\ UFR)(ULF\ URB)$. When I apply this algorithm, I usually begin with my red-blue edge cubelet in its proper position, and then I repeat the algorithm until the yellow-blue edge cubelet is properly placed. Then, if I need to, I rotate the whole cube so that I’m looking at the white face, I repeat the algorithm one more time from that position, and then I rotate the up face $90^\circ$ clockwise, and I’m done. Notice, too, that if we did this algorithm three times, then the result would be $(UBL\ UFR)(ULF\ URB)$ which means that we are just switching, on the up face, two back corner cubelets diagonally with two front corner cubelets. Again, this, in itself, could be a useful algorithm for an alternate solution to Rubik’s cube.
At this point, we just need to permute our corner cubes using the algorithm $URU^{-1}L^{-1}UR^{-1}U^{-1}L$. Embedded in this algorithm we can see the conjugates $URU^{-1}$ and $(L^{-1}U)R^{-1}(U^{-1}L)$. Also, if we removed all the turns of the up face from this algorithm, then we would be left with the commutator $RL^{-1}R^{-1}L$, but by itself this algorithm equals the identity since $R$ and $L$ commute with one another. Hence, we need the rotations of the up face thrown in order to achieve something meaningful. And all that this algorithm wonderfully does is to permute three corner cubelets on the up face, $(ULF\ URB\ UBL)$. Usually, you want to turn your cube so that the corner cubelet in the up-right-front position is already properly placed. If none of the corner cubelets are in their correct position, then just perform this algorithm once, and you should be able to find one that you can make the up-right-front cubelet just by turning the whole cube. And from there, just keep repeating the algorithm until all the corner cubelets on the up face are in their correct positions. As before, if you perform these algorithms step by step in the software program Rubik, then it’s a lot easier to see what’s going on!
Our final move is to simply rotate the corner cubelets on the up face until they get the proper orientation and the cube is solved. To do this, we use the algorithm \((R^{-1}D^{-1}RD)^2\).

Notice that the core of this algorithm is the commutator \(R^{-1}D^{-1}RD\), and the cycle structure for this algorithm is \((DB\ DR\ FR)\). The good news is that this algorithm leaves the up-right-front cubelet right where it is, and when we perform it, we also see that it rotates the up-right-front cubelet 120° counterclockwise which is equivalent to a clockwise rotation of 240°. The bad news, of course, is that it messes up the rest of the cube. However, since we have a cycle of length 3, that means that if we perform the algorithm three times, then nothing is left messed up. Now here’s the cool part. Remember that in our earlier chapter on counting the number of permutations in Rubik’s cube we saw that every turn of a face would collectively rotate our corner cubelets some multiple of 360°. Well, that means that when we get down to this final point in solving the cube, our last four corner cubelets are collectively going to be rotated by some
multiple of 360°, and since each application of \((R^{-1}D^{-1}RD)^2\) results in a rotation of the up-right-front corner cubelet by 120° counterclockwise, the number of times we’re going to have to perform this algorithm is going to be some multiple of three, and thus, in the end none of the rest of the cube will be disturbed. Hence, we position a corner cubelet that needs to be rotated in the up-right-front position and apply \((R^{-1}D^{-1}RD)^2\) until its right, and then we move another corner cubelet on the up face into that position and apply \((R^{-1}D^{-1}RD)^2\) again until it’s correctly oriented. And the end result is that our cube is solved. And it’s just that simple!
Rotate the up face and apply \( (R^{-1}D^{-1}RD)^2 \) twice.

Stick a fork in it, it's done!
The main goal of this book has been to introduce you to some of the joys and techniques of group theory and to make traditional, abstract algebra more concrete by relating it to Rubik’s cube. However, now that we have covered quite a bit of material, there are some other things I want you to realize. In particular, I hope you recognize that groups are everywhere! For example, anytime you come across cycles or permutations or symmetry in life, there is going to be a corresponding group!

Cycles are something we should see quite easily in our lives. For example, we wake up, we get dressed, we go to work, we come home, we go to sleep, and then the next day this cycle usually repeats itself. This results in a very simple cyclic group that most of us experience on a daily basis. Also, throughout the day we pass by others who are engaged in their own cycles, and if their cycles are disjoint from ours, then they will commute with us, and what one of us does won’t affect the other. However, some days we encounter a book or a person or some other situation that brings a new cycle into our lives. When we encounter that person, their cycles may not be entirely separate from ours, and then our cycles start to combine with theirs in new and complex ways that are not so independent of one another. And remember that all groups are the product of the ways in which elementary cycles combine and interact with one another.

My life is not only filled with repetitive cycles, it’s also replete with symmetry, and by symmetry I simply mean any type of pattern which is repeated. For example, I walk into
a classroom, and I see row after row of identical desks. That’s symmetry! And corresponding to that symmetry there will be a mathematical group! I look at every human being I encounter, and I see bilateral symmetry that can mathematically be described by the group of integers modulo 2, \( \mathbb{Z}_2 \). I look at buildings and logos and streets and plants, and everywhere I look I see symmetry. And that means that everywhere I look there are groups that describe the symmetry I am experiencing. There are also patterns of behavior in my life that I repeat, and those behavioral patterns are also a type of symmetry that may be described by groups.

As an example, following this paragraph is a picture of my fireplace. The square shape reminds me of \( D_4 \), the symmetries of the square. The eighteen square pieces of stone surrounding the fireplace bring to mind \( \mathbb{Z}_{18} \), the cyclic group of order 18, as well as \( D_4 \) again. The rectangular wooden beam at the top has two axes of symmetry, one vertical and one horizontal, and associated with this symmetry is \( \mathbb{Z}_2 \oplus \mathbb{Z}_2 \), the Klein four-group. And finally, the guitar in the picture exhibits bilateral symmetry (\( \mathbb{Z}_2 \)), and the six strings on the guitar suggest both \( \mathbb{Z}_6 \), the cyclic group of order 6, and \( S_6 \), the group of all permutations to be made from six objects. As you can see, we can go on and on identifying symmetries and their corresponding groups! And don’t even get me started talking about the symmetries of the curtains and the floor tiles! Groups and symmetry are everywhere!
Permutations also play a large role in our lives. For example, I often say that the only difference between a messy room and a clean room is how things are arranged. Whether we are cleaning our room or mowing the lawn or arranging the furniture, we are just making a different permutation of what’s already there. Some philosophers like to refer to these permutations of existing objects as *something from something creation*. In other words, we are just taking things that already exist and creating a different arrangement of them. Also, it’s likely that much of your daily life is spent making permutations of one sort or another. For instance, you might spend a lot of your day filing papers, organizing mail, cleaning rooms, doing yard work, or processing orders, and what all of these
activities have in common is that they all involve generating permutations of the existing reality. They are all *something from something creation*.

One of the last things I talked about were quotient structures, and I want to talk more about this topic now and expand it beyond the confines of just group theory. The quotient structure is one of those concepts that permeates all of mathematics, and, in a sense, it results in a change in our reality as a consequence of us suddenly seeing things that we previously had considered distinct as now being equivalent. For instance, when we look at the integers, at some point we realize that we can group all the numbers divisible by 2 together, and that creates a new reality with just two objects, *even* and *odd*. To give a geometric example, think of having a piece of string with two ends that we’ll call $A$ and $B$. 

![Diagram of a piece of string with two ends labeled A and B]
If we now attach the two endpoints together, i.e. make $A = B$, then we create a new object, a circle.
We can think of this new reality as a quotient structure that has been brought about by making $A$ equivalent to $B$. In a similar manner, we can transform a piece of paper into a cylinder by making the edges of two opposing sides equivalent to one another, and then we can transform the cylinder into a bagel or donut (what mathematicians call a torus) by equating the opposite ends of the cylinder. All of these are examples of creating something new via quotient structures.

I now claim that every time we have an epiphany or insight or “aha!” moment, we are actually creating a new quotient structure for ourselves. For example, you did not always see the world as you do today. You had to learn that the letters “t-h-e” come together to form the word “the.” You had to learn that trees come together to form a “forest.” And you had to learn that various pieces of wood come together to form what you now easily recognize as a “chair.” In other words, at one point in your life, none of these things happened automatically. You literally had to figure out for yourself how objects and ideas somehow combine to form other things, and when you do this, it’s really a quotient structure because components that were previously seen as unrelated now become
connected in the new reality, and whatever was previously keeping these things apart has been divided out in the quotient structure. Some would call this *something from nothing creation* because we are literally creating new worlds for ourselves, seemingly out of nothing, by combining things into equivalence classes, and thus, the pieces of wood that at first seemed unrelated now find equivalence in a new concept called “chair.”

Well, so much for grand philosophizing. The point, however, is that cycles, patterns, permutations, symmetry, and groups are all around us, and we now want to go through our days with an increased awareness of them. As we do so, we can also engage in what I call *something from something creation* and *something from nothing creation* by either rearranging our world to make it better or by gaining new insights into things through a process that I see as identical to forming quotient structures. Either way, recognize that groups are everywhere, and live a creative life!¹

¹ For a more detailed discussion of my cognitive interpretations of quotient structures, see “Algebraic Models for Constructivist Theories of Perception” at [www.docbenton.com](http://www.docbenton.com).
Symmetry is everywhere!
Christopher Benton is from parts unknown and grew up Deep in the Heart, Texas. After many adventures and misadventures, he finally became an adult and obtained a master of science degree and a doctor of philosophy degree in mathematics from the University of Houston. He currently lives in Arizona in The Valley of the Sun with his beloved wife, Susan, and their dog, Dr. Chloe Continuum, Do.G. (doctor of growlology). Chloe’s favorite pastimes are eating tasty dog food and curling up every evening with a good calculus book to read. Doc Benton occasionally, once in a blue moon, whenever he feels like it, reads and responds to email sent to docbenton@docbenton.com.

Compliments and information about typos and other errors are welcome. Whiners, though, will be punished!