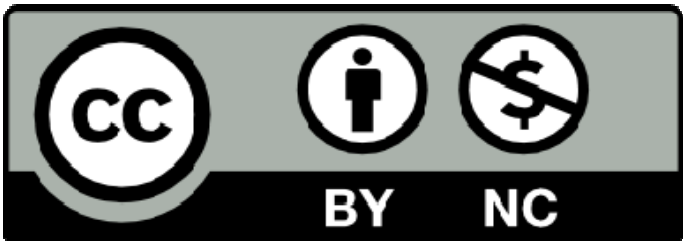
A CHILD'S GARDEN OF GROUPS

An introduction to the mathematical theory of groups for young and old!

(Part 1)

by

Doc Benton



Creative Commons License

You are free to:

- Share this work
- Adapt this work
- Attribute all original materials to Doc Benton

You are not free to:

- Charge money for this work; Knowledge is free!

CONTENTS (PART 1)

INTRODUCTION (PART 1)

Welcome! This is Part 1 of an introduction to *group theory* that will ultimately be comprised of ten different parts ranging from the absolute beginning to very advanced! *Group theory* (of course!) is a part of higher, abstract algebra, and this first part primarily introduces the concept of a mathematical *group* and illustrates how *groups* are connected with not only the various cycles in our lives, but also symmetry and permutations. Also, in order to make each chapter as brief as possible, often only a single example of a concept is given. However, many more examples are given in subsequent parts.

In subsequent parts of this book, we'll continue to introduce some of the basic concepts, examples, and ideas of *group theory*, but most of these parts will not contain any proofs. Instead, we'll try to provide some hands-on practice and illustration by introducing you to Rubik's cube and to a free software program called GAP (*Groups, Algorithms, and Programming*). Eventually, we will introduce you, in Part 9, to theorem proving via some of the easier and shorter proofs that one may find in a standard *group theory* course, and then in Part 10 we will show you some lengthier and more advanced theorems that are very fundamental to *group theory*. I hope many of you make it that far!

Group theory is a branch of mathematics that most people have never heard of, and yet it is of fundamental importance to of mathematics and physics. In fact, one of its first applications in advanced mathematics was to prove that it is impossible to construct a general formula for solving all polynomial equations of degree 5 or higher. In particular, there is no convenient formula for solving 5th degree equations that look like $a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0$ where we have an *x* to the 5th power term, but no higher. Likewise, there is no general formula for solving all 6th degree polynomial equations, equations that look like

$a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0$ where there is an *x* to the 6th power term, but no higher. And more generally, for $n \geq 5$ there is no convenient formula for solving all equations of the form $a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_2x^2 + a_1x + a_0 = 0$.

Those who have successfully completed a basic algebra course will undoubtedly have seen the quadratic formula, $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$, for solving polynomial equations of degree 2 such as $ax^2 + bx + c = 0$, but once we get to powers of 5 or larger in our equation, no such general formula exists. Note, however, that formulas do exist for solving cubic polynomial equations and polynomial equations of degree 4, but because of their complexity, they are rarely taught in basic algebra courses.

Group theory has many important applications besides the one given above, and, in particular, it is the mathematical tool of choice whenever symmetry or permutations are involved. That not only makes it the mathematics of modern particle physics where often all that physicists have to work with are symmetries at the subatomic level, but also the mathematics behind Rubik's cube. Additionally, once we give the algebraic definition of a *group*, we'll see that many of the things we study in mathematics are examples of *groups*, and consequently, a single theorem about *groups* can apply to many, many different areas of mathematics. Thus, my ultimate goal is to give you a sense of what a *group* is within the context of mathematics and an understanding that examples of *groups* are all around us. Any difficulties that arise in this first part will likely be due not to the inherent difficulty of the subject, but rather to the fact that new concepts and ideas are suddenly being thrust upon you. Nevertheless, persevere, and you will be greatly rewarded. You will learn to see the world through new eyes, and you will see a world filled with cycles and symmetry and endless rearrangements of creation!

WHAT IS A GROUP?

What is a *group*? Well, that's a very good question! First and foremost, a *group* is a collection of objects that satisfies a small list of algebraic properties. Also, in mathematics we usually call any well-defined collection a *set*, and this term is used for collections even in plain English such as when we talk about a *set of china*. The word *group* can also refer in plain English to some kind of a collection, but in mathematics we only use this word when our collection satisfies particular algebraic properties. Thus, I guess the next thing to do is to explain what those properties are!

The first property is called *closure*, and this is what it means. First, there has to be something in our *set*, at least one element, because otherwise things are going to be pretty boring if we are just looking at a totally *empty set*, a collection of nothing. And second, given any two elements from our *set* (not necessarily distinct from one another), there has to be a way of combining them in order to get back something that is once again in our *set*. That's why this property is called *closure*, because a *set* with such an operation defines a closed system. In other words, combining any two elements together doesn't take us anyplace other than to just another element in our *set*. Furthermore, when we have a closed operation that combines two elements to give us back something in our original *set*, we call this a *binary operation* since *binary* means *two* and two elements are being combined. When we are dealing with numbers from our familiar number system, the most commonly encountered *binary operations* are our familiar addition, subtraction, multiplication, and divison $(+,-,\cdot,\div)$. However, if we are just talking about *binary operations* more abstractly, then we might use a symbol like "$*$" to represent that operation, or we might also just use addition, multiplication, or juxtaposition of elements in order to indicate a *binary operation*.

Consequently, if elements *a* and *b* are being combined, then it might be written as $a*b$ or $a+b$ or $a\cdot b$ or simply as ab.
The next property a *group* has to have is *associativity*, and that means that we can group things with parentheses or other grouping symbols in any way we like without changing the outcome. This property is usually stated in the form $(a*b)*c=a*(b*c)$. This property holds, for example, for our usual addition or multiplication of numbers.

The third property of a *group* is the existence of an *identity element*. What this means is that we have an element in our *set* that acts either like the number 0 under addition or like the number 1 under multiplication. For instance, when you add 0 to a number, you don't change that number's identity, and when you multiply a number by 1, again you don't change that number's identity. When dealing with a *group*, some commonly used symbols for the *identity element* are 0, 1, *e*, or even $(\ )$. This latter symbol is commonly used in the free computer program called GAP (*Groups, Algorithms, & Programming*) that we'll talk about later. The *identity property* is generally expressed by the equation $e*a=a=a*e$.

The fourth and final property of a *group* is the *existence of inverses*. In arithmetic, an *inverse* is something which undoes what you just did. For example, to undo adding 3 to something, you can just add -3, and to undo multiplying by 2, you can follow that with a multiplication by $2^{-1}=1/2$. Notice, too, that in addition $3+(-3)=0$ and in multiplication $2\cdot 2^{-1}=2\cdot\frac{1}{2}=1$. In other words, in a *group*, combining an element with its *inverse* always gives us back the *identity*.

Some very important *groups* have a fifth property called the *commutative law* that is written as $a*b=b*a$. In plain English, the word *commute* denotes something traveling or moving around, and, thus, the *commutative law* (or *property*) says that when we combine things, it doesn't matter what order we write the elements down in. We can move them around, if we want to, without changing the final

result. Additionally, when we know that a *group* is *commutative,* it is often customary to use additive notation such as $a+b=b+a$. And furthermore, a *commutative group* is also known as an *abelian group*. This name is in honor of the Norwegian mathematician Niels Henrik Abel (1802-1829) who was one of the founders of *group theory*. Notice that he didn't live very long, only 27 years. Nonetheless, take a moment to honor his life by reading about him in the Wikipedia. And who knows? Maybe future generations will honor your life by reading about you in the Wikipedia long after you are gone!

Now let's look at a formal definition of a *group* that incorporates everything we've been discussing.

Definition: A *group* is a *nonempty set* of objects *G* with a *binary operation* $*$ defined such that the following algebraic properties are present:

1. (*closure*) If a and b are elements of *G*, then $a*b$ (read as either "a star b" or "a times b") is an element of *G*.

2. (*associative law*) If a, b, and c are elements of *G*, then $(a*b)*c=a*(b*c)$.

3. (*existence of an identity element*) There exists an element e in *G* such that if a is any element in *G*, the $e*a=a=a*e$.

4. (*existence of inverses*) If a is any element in *G*, then there exists an element a^{-1} (a-inverse) in *G* such that $a*a^{-1}=e=a^{-1}*a$.

If, in addition to the above, the following fifth property is also satisfied, then we call our *group* an *abelian* or *commutative group*.

5. (*commutative law*) If a and b are elements of *G*, then $a*b=b*a$.

For convenience, mathematicians usually just write ab or $a\cdot b$ (instead of $a*b$) if we are talking about either *groups* in general or *nonabelian groups* in particular, and we write $a+b$ to denote the *binary operation* in an *abelian* or *commutative group*. In our next chapter, we'll look at some familiar examples of *groups*!

EXAMPLES OF GROUPS

The first examples of *groups* that we'll give are those that we encounter in basic arithmetic. In particular, the first example we'll consider is the set of *integers* under addition. Two things to notice here, though. First, we have to specify not only a *set* of objects, but also the operation that will be used to combine those objects. Thus, in this case the operation is just the usual addition that we do with numbers, and the *set* of objects, the *integers*, is the *set* of those numbers that we usually mark off for our scale on the *number line*. In other words, $\{\ldots,-2,-1,0,1,2,\ldots\}=\{0,\pm1,\pm2,\ldots\}$. We usually denote this *set* by a block letter *z* written as $\mathbb{Z}=\{\ldots,-2,-1,0,1,2,\ldots\}=\{0,\pm1,\pm2,\ldots\}$. The origin of this notation is the German word *zahlen* which means *numbers*.

So, to continue, the claim is that *integers* under the operation of addition, written more formally as $(\mathbb{Z},+)$, form a *group*. In this *group*, the *identity element* is 0 since for any *integer a* we have that $a+0=a=0+a$, and the *inverse* of a is its opposite, $-a$. Hence, for example, the *inverse* of 2 in this *group* is -2, and the *inverse* of -2 is $-(-2)=2$, and we can easily see that $2+(-2)=0$ and $-2+\left[-(-2)\right]=-2+2=0$. Also, it's easy to convince ourselves that the sum of two *integers* is an *integer* (*closure*) and that the *associative law* holds as in the case, for example, of $3+(2+1)$ and $(3+2)+1$. In the first instance we have $3+(2+1)=3+3=6$, and in the second instance we have $(3+2)+1=5+1=6$, thus verifying that $3+(2+1)=(3+2)+1$. Hence, since we have a *nonempty set* along with an operation for combining the elements of that *set*, and since this operation exhibits *closure*, *associativity,* an *identity element,* and the *existence of inverses*, it follows that $(\mathbb{Z},+)$ is a *group*. Furthermore, it's an *abelian* or *commutative group* since, as we know, it doesn't matter what order we add these numbers in. We always have that for any two *integers* a and b, $a+b=b+a$.

To see a *set* of ordinary numbers that do not form a *group*, we need look no further than $(\mathbb{Z},-)$, the *integers* under the operation of subtraction. To show that this is not a *group*, it suffices to exhibit that the *associative property* is not always valid under this operation. Thus, for example, consider $3-(2-1)$ and $(3-2)-1$. If we reduce the expression on the left, we get $3-(2-1)=3-1=2$, but if we reduce the expression on the right, we get $(3-2)-1=1-1=0$ which is different. Thus, the *associative law* doesn't hold in $(\mathbb{Z},-)$, and this is not a *group*.

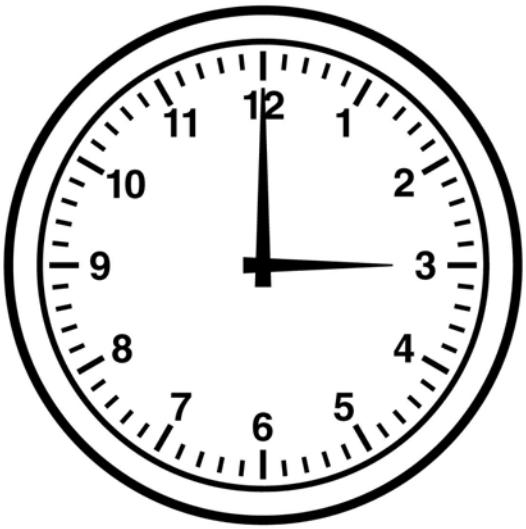
Some other examples of *groups* include $\left(\mathbb{R}^+,\cdot\right)$, $(\mathbb{Q},+)$, $\left(\mathbb{Q}-\{0\},\cdot\right)$, $\left(\mathbb{R}-\{0\},\cdot\right)$ and $(\mathbb{R},+)$. Now let me explain some of the notation. The symbol $\mathbb{R}^+$ stands for the *positive real numbers* (the numbers on the *number line* that are greater than zero), $\mathbb{Q}$ stands for the *rational numbers* (numbers that you can write as a ratio of two *integers*), and $\mathbb{R}$ stands for the *real numbers* (all the numbers on the familiar *number line* and so named because we think of them as the kinds of numbers that describe the real world). Additionally, $\mathbb{Q}-\{0\}$ means *all rational numbers except for 0*, and $\mathbb{R}-\{0\}$ means *real numbers except for 0*. And now that we understand the notation, we can describe the *groups* listed above as:

- $\left(\mathbb{R}^+,\cdot\right)$ = the set of *positive real numbers* under multiplication
- $(\mathbb{Q},+)$ = the set of *rational numbers* under addition
- $\left(\mathbb{Q}-\{0\},\cdot\right)$ = the set of *nonzero rational numbers* under multiplication
- $\left(\mathbb{R}-\{0\},\cdot\right)$ = the set of *nonzero real numbers* under multiplication

Just from these few examples, you can probably get the idea that *groups* exist throughout mathematics, and thus, any single theorem that we prove about *groups* will apply to many different situations!

CLOCK ARITHMETIC

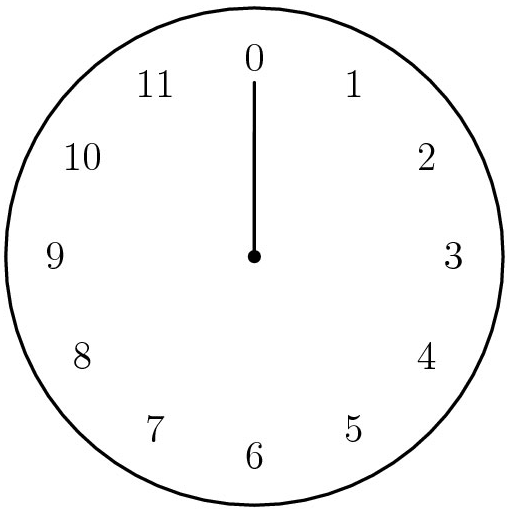
Most of you probably learned about “clock arithmetic” in elementary school. It’s basically like ordinary addition of *integers* except that when you get to twelve, you start over. For example, let’s consider the image below.



The time shown on this clock is 3 o’clock. And if we add 9 hours to that, then we get 12 o’clock. So far it’s just like saying that $3+9=12$. However, if we add 10 hours to 3 o’clock, then we don’t wind up with 13 o’clock. Instead, we start over after 12 and wind up at 1 again. Hence, in clock arithmetic we say that $3+10=1$, and an easy way to compute this result is to first compute $3+10=13$ and then look at the remainder when we divide this result by 12, $\begin{array}{r} 1, \text{remainder } 1 \\ 12\overline{)\,13} \end{array}$. Thus, with clock arithmetic we obtain results like the following:

$3+1=4$
$3+2=5$
$3+3=6$
$3+4=7$
$3+5=8$
$3+6=9$
$3+7=10$
$3+8=11$
$3+9=12$
$3+10=1$
$3+11=2$
$3+12=3$

Again, we can think of it in the sense that once we reach 12, everything just wraps around back to the beginning. Also, observe that in clock arithmetic, $3+12=3$ and $12+3=3$. This means that 12 acts like the number 0, an identity element, and hence, mathematicians find it more convenient to use a clock that has 0 at the top instead of 12.



Consequently, our previous addition table now looks like the following:

$3+1=4$
$3+2=5$
$3+3=6$
$3+4=7$
$3+5=8$
$3+6=9$
$3+7=10$
$3+8=11$
$3+9=0$
$3+10=1$
$3+11=2$
$3+0=3$

Mathematically, we like to say that we are doing arithmetic with the set of numbers $\{0,1,2,3,4,5,6,7,8,9,10,11\}$, and the addition is just like ordinary addition except that when we add 1 to 11, we just wrap around back to 0. Also, mathematicians call this type of clock arithmetic "*addition modulo* 12." Furthermore, the set $\{0,1,2,3,4,5,6,7,8,9,10,11\}$ with *addition modulo* 12 gives us another example of a *group*, and since this *group* wraps around in a cycle, we call it a "*cyclic group*." Additionally, since this *group* contains only a finite number of elements, it is, in particular, a *finite cyclic group*, and we can generate the entire *group* by repeatedly adding 1 to itself until we get back to 0 and then adding 1 any further just causes the cycle to repeat. And lastly, there are two common notations for this *group* called the *integers modulo* 12. We can denote it either as $\mathbb{Z}_{12}$ ($\mathbb{Z}$ for *integers*) or as C_{12} (*C* for *cyclic*).

CYCLIC GROUPS

In our last lesson we discussed clock arithmetic and how when we add the numbers in the set $\{0,1,2,3,4,5,6,7,8,9,10,11\}$ using clock arithmetic, then the results eventually wrap around to the beginning, i.e. 0, and repeat themselves. At this point, there are now several things that we should point out:

- The above set coupled with the clock arithmetic procedure for combining elements gives a *group* that we can call either the *integers modulo* 12, denoted by $\mathbb{Z}_{12}$, or the *cyclic group of 12 elements*, denoted by C_{12}.
- We call the number of elements in a *group* the *order of the group*, and in this case, C_{12} is a *cyclic group* of order 12.
- The first *groups* we looked at like the *integers* under addition, $(\mathbb{Z},+)$, and the positive real numbers under multiplication, $(\mathbb{R}^+,\cdot)$, are examples of *infinite groups* (*groups* of *infinite order*, an infinite number of elements), but $\mathbb{Z}_{12}$ (or C_{12}) is an example of a *finite group* (a *group* of *finite order*, a finite number of elements).
- All of the elements of the *group* $\mathbb{Z}_{12}$ can be generated by adding 1 to itself over and over as indicated below.

$1=1$
$1+1=2$
$1+1+1=3$
$1+1+1+1=4$
$1+1+1+1+1=5$
$1+1+1+1+1+1=6$
$1+1+1+1+1+1+1=7$
$1+1+1+1+1+1+1+1=8$
$1+1+1+1+1+1+1+1+1=9$
$1+1+1+1+1+1+1+1+1+1=10$
$1+1+1+1+1+1+1+1+1+1+1=11$
$1+1+1+1+1+1+1+1+1+1+1+1=0$

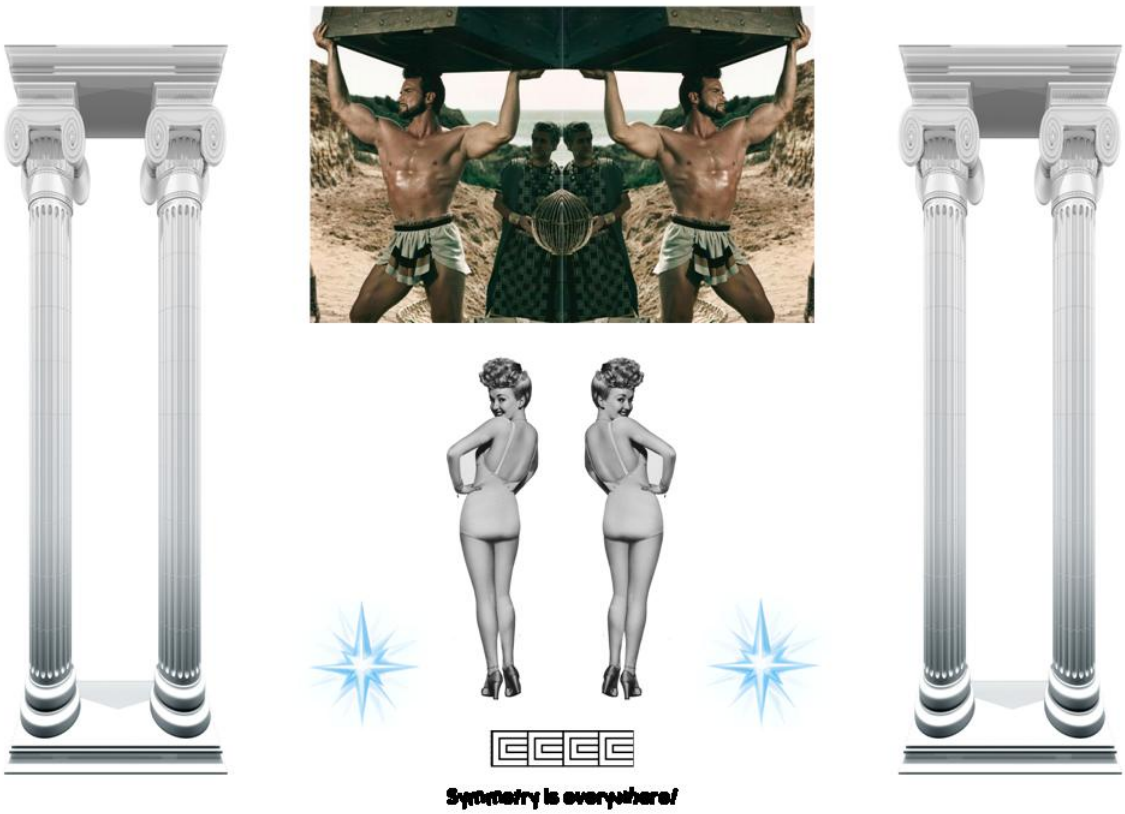
- We often like to express a *group* in terms of the products (or sums) of a minimal *set* of elements whose products (or sums) will generate the entire *group*. And in general, any such *set* of elements that can be used to generate the entire *group* we simply call *generators for the group*. Furthermore, even though 1 is the obvious choice for a *generator* for $\mathbb{Z}_{12}$, it's not the only single element that can generate this *group*. We can also generate this *group* by adding 5 to itself over and over. Just remember, though, that when we do *addition modulo* 12, the result is whatever the remainder is when, first, we add the numbers together using regular arithmetic and then, second, we divide by 12 to see what remainder we get. This results in the following table that shows that every number in our set $\{0,1,2,3,4,5,6,7,8,9,10,11\}$ can be found by adding 5 to itself repeatedly.

$5=5$
$5+5=10$
$5+5+5=3$
$5+5+5+5=8$
$5+5+5+5+5=1$
$5+5+5+5+5+5=6$
$5+5+5+5+5+5+5=11$
$5+5+5+5+5+5+5+5=4$
$5+5+5+5+5+5+5+5+5=9$
$5+5+5+5+5+5+5+5+5+5=2$
$5+5+5+5+5+5+5+5+5+5+5=7$
$5+5+5+5+5+5+5+5+5+5+5+5=0$

- For any counting number *n* we can talk about the *group of integers modulo n*, $\mathbb{Z}_n$, which is essentially the same thing as the *cyclic group* of order *n*, C_n.
- Cycles appear everywhere in our lives, and that means that *groups* also appear everywhere in our lives!

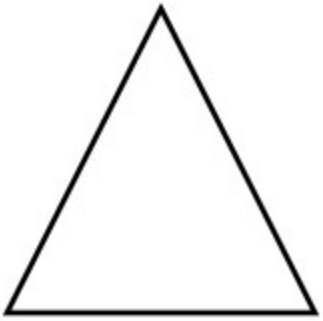
SYMMETRY

Symmetry is just a pattern that is repeated in some way, and when a pattern is repeated, then there is always some movement or operation that can be performed to transform one instance of the pattern into another instance. For example, consider the picture below.

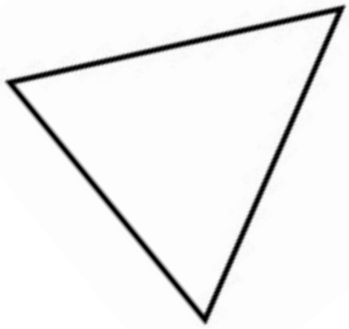


In this image you see a lot of *mirror symmetry* that is created by reflecting a picture across either a vertical or horizontal axis. Likewise, the human body itself has *bilateral symmetry* in that the right side of our body is just the mirror image of the left side reflected across a vertical line. However, whether we are looking at our own *bilateral symmetry* or the mirror images above, in each case we can see

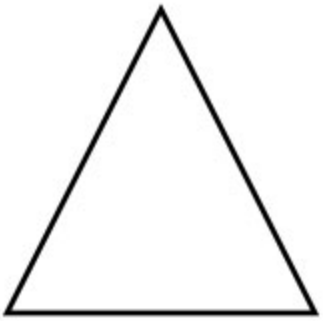
patterns that are repeated. Now let's look at another example, the *rotational symmetry* of an equilateral triangle (a triangle with three equal sides).



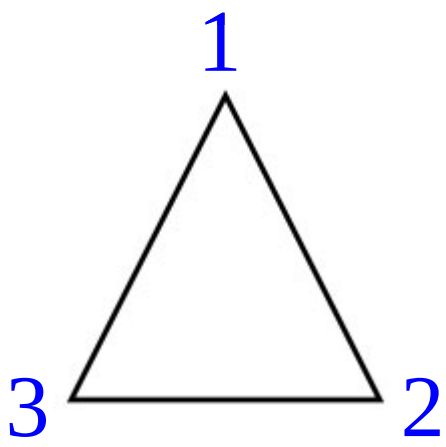
Notice that if we rotate this triangle about its center approximately $45°$ in the clockwise direction, then it doesn't look the same as what we started with.



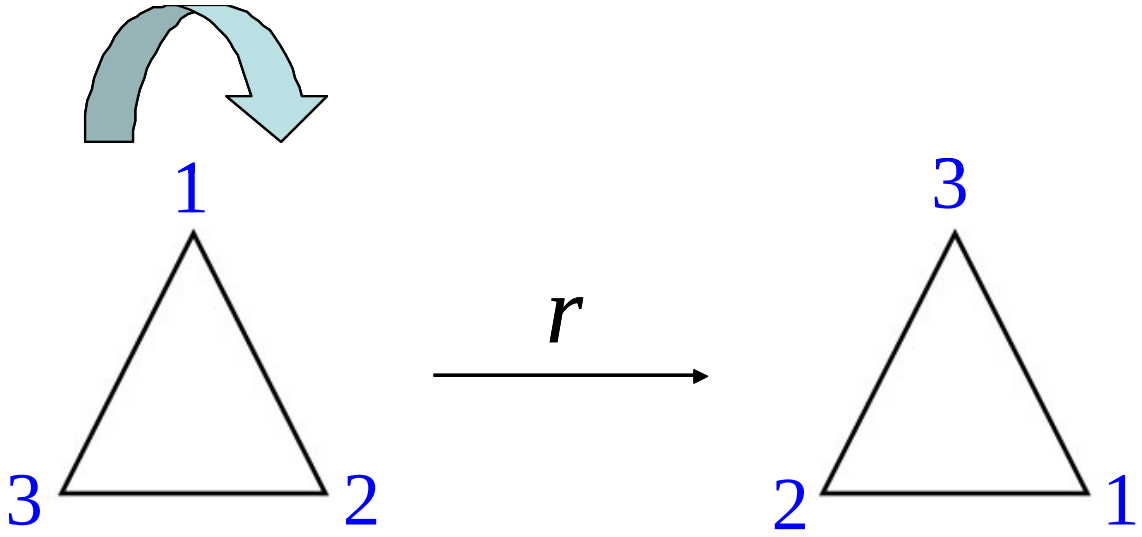
However, if we rotate it clockwise either $120°$ or $240°$, then it will look exactly the same as our beginning triangle. This is the type of rotation that reveals a *symmetry* within our triangle.



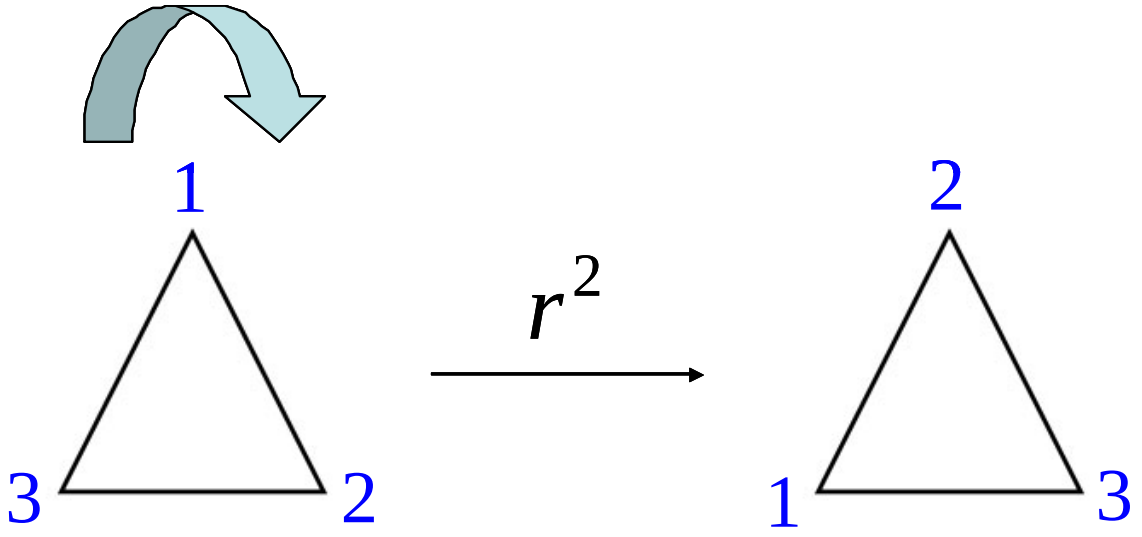
To better see what's going on when we do this rotation, we can number the vertices of the triangle and follow their motion.



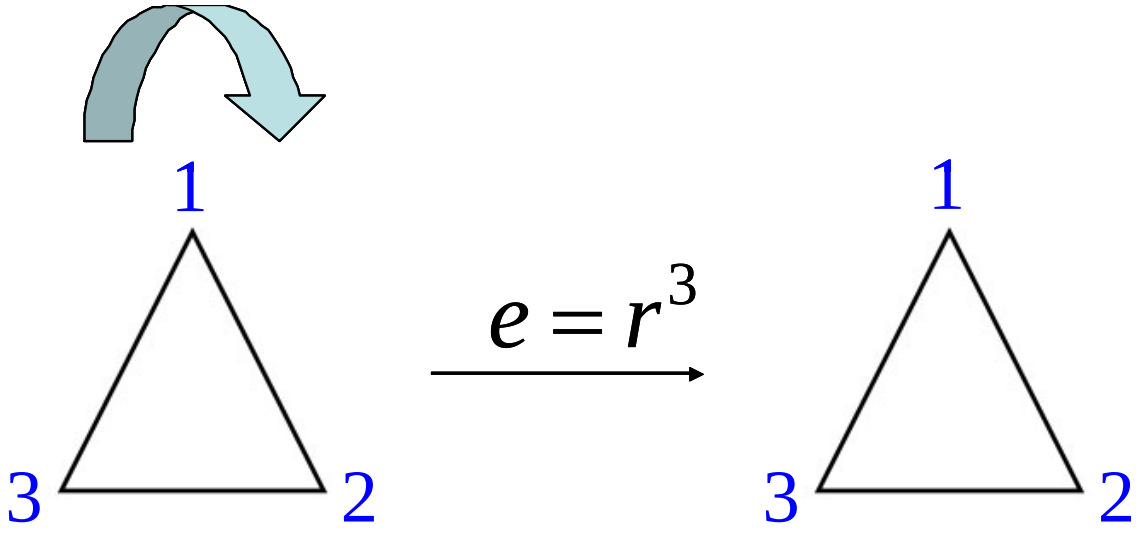
If we let *r* represent a clockwise rotation of $120°$ about the center, then the diagram below shows the effect on the vertices of the triangle.



If we rotate our original triangle $240°$ clockwise, then that would be like doing *r* twice, and so we'll write that as r^2.



And finally, if we do a clockwise rotation through $360°$, then the end result is just as if we hadn't done any rotation at all. Changing nothing, doing no rotation at all, corresponds to the identity element which we traditionally represent by the letter *e*. Hence, regarding our rotations, we basically have $e = r^3$.



Thus, what has happened is that the *rotational symmetry* of the equilateral triangle has led us to discover a geometric representation of the *cyclic group of order 3*. The distinct elements of this *group* are $\{e, r, r^2\}$.

We could likewise examine the *rotational symmetry* of a square to discover a *cyclic group of order 4* or a regular pentagon (a pentagon with 5 sides of equal length) to discover a *cyclic group of order 5*. The most important point to be made, however, is that wherever symmetry is present, there is going to also be present a *mathematical group* whose elements consist of those operations that appear to leave the underlying object unchanged.

MULTIPLICATION TABLES

Let's go back and revisit $\mathbb{Z}_3$, the *integers modulo* 3. The elements of this *group* are given by the *set* $\{0,1,2\}$, and the operation is ordinary addition with the restriction that anything larger than 2 has to wrap around in order to give us a final result of either 0, 1, or 2. Also, since this *group* has only three elements, we can easily construct an addition table for this *group*. However, note that the generic term in *group theory* for any such table is "multiplication table." Thus, here is the "multiplication table" for the *integers modulo* 3.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

From this table, we can easily see the various results of doing *addition modulo* 3 such as $1+1=2$, $1+2=0$, and $2+2=1$. Also, below we have highlighted in orange in our table the diagonal going from upper left to lower right, we've highlighted in green a lower triangle, and we've highlighted in yellow an upper triangle.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Notice that the lower green triangle looks like the mirror image of the upper yellow triangle. This is what happens in a multiplication table whenever the *group* is *commutative* (*abelian*). Hence, it does not matter what order the elements are added in. Thus, for example, $1+2=0=2+1$.

Now let's look at the multiplication table for the *cyclic group* we found in the last chapter that represented the *rotational symmetry* of an equilateral triangle.

$\cdot$	e	r	r^2
e	e	r	r^2
r	r	r^2	e
r^2	r^2	e	r

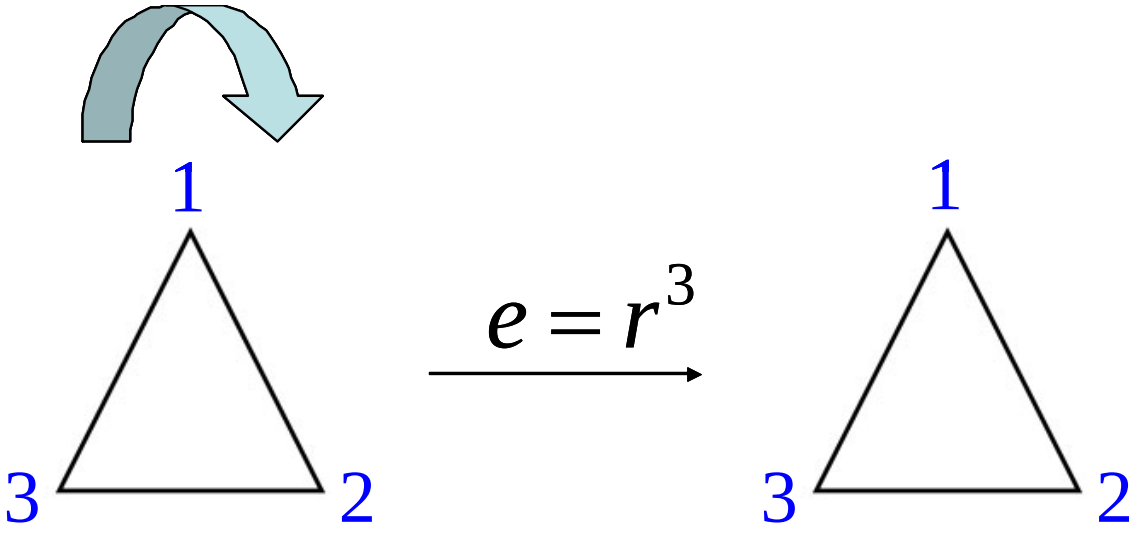
Notice how similar this table looks to the one we constructed for $\mathbb{Z}_3$. In fact, if we make the substitutions indicated below, then we can realize that the two tables are identical except for the symbols used to represent our elements.

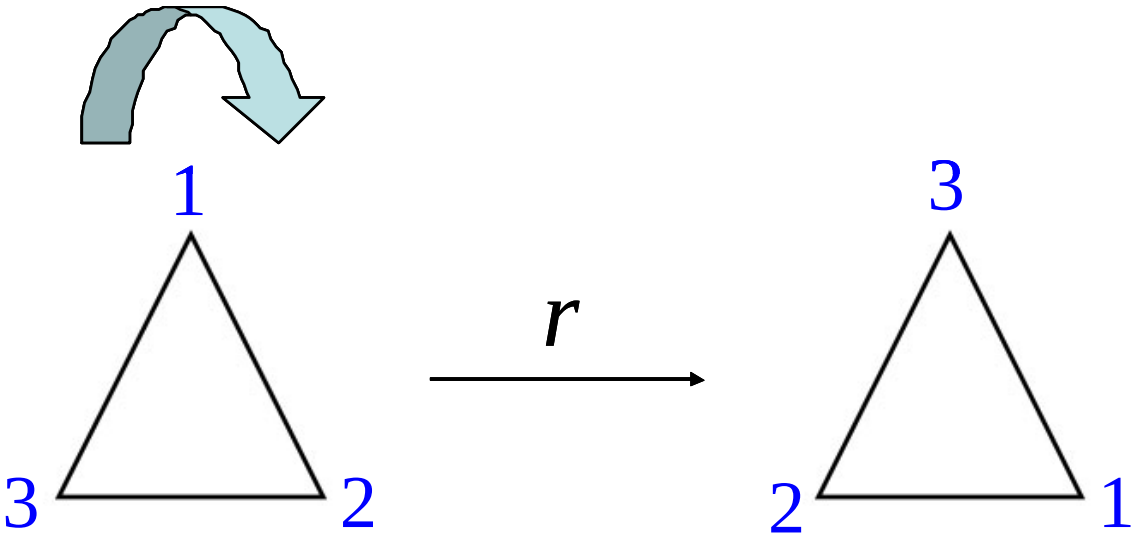
$$\begin{aligned} 0 &\leftrightarrow e \\ 1 &\leftrightarrow r \\ 2 &\leftrightarrow r^2 \end{aligned}$$

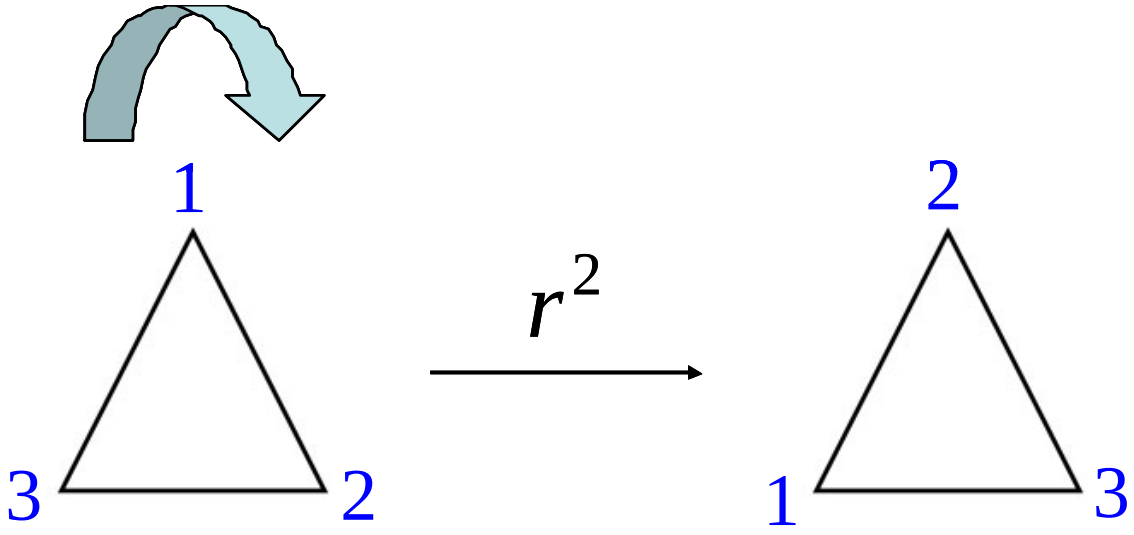
Furthermore, whenever two *groups* can be represented by multiplication (or addition) tables that are identical except for the symbols used, then we say that the two *groups* are *isomorphic*. That word means "equal shape," and most of the time we won't make any distinction between *groups* that are *isomorphic*. In particular, we will normally treat the *integers modulo* 3, $\mathbb{Z}_3 = \{0,1,2\}$; our *rotation group* for the equilateral triangle, $R = \{e, r, r^2\}$; and the *cyclic group* of order 3, $C_3 = \{e, a, a^2\}$, as identical since they are all *isomorphic* to one another. They are all simply different ways to represent a *finite cycle of length 3*.

PERMUTATIONS

Previously, we explored the *symmetry* of an equilateral triangle by labeling the vertices 1, 2, and 3, and we then followed what happened as we rotated our triangle clockwise through angles that are integer multiples of $120°$. The pictures below illustrate the results.



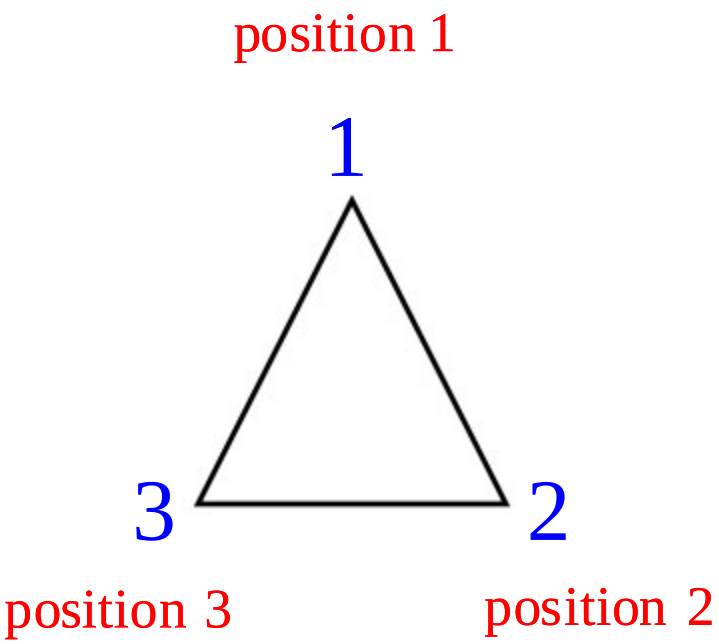




Notice that the end results can also be described in terms of permutations of the numbers 1, 2, and 3 where by a *permutation* we mean an arrangement in which order makes a difference. Thus, starting at the top of our triangle and moving clockwise, we could say that the first rotation through $120°$ (r) changes the arrangement 123 to 312, while a rotation of $240°$ (r^2) from our starting point changes 123 to 231. Likewise, a rotation of $360°$ (r^3) leaves 123 as 123, and thus, it is equivalent to *e*, the *identity element*.

A common way to indicate a permutation is by drawing arrows to show what each object or number changes to. For example, in our first rotation through $120°$ (r) we often say that 1 goes to 2, 2 goes to 3, and 3 goes to 1, and we can write the permutation like this, $\begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{pmatrix}$. However, even though we commonly say 1 goes to 2 and so one, we actually mean something a little different. In particular, think of the vertex at the top of our triangle as *position 1*, the vertex at the bottom right as *position 2*, and the vertex at the bottom left as *position 3*. Then what we

really mean to say by $\begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{pmatrix}$ is that the number currently in position 1 is moved to position 2, the number currently in position 2 is moved to position 3, and the number currently in position 3 is moved to position 1



With that cleared up, we can now express our three rotations as the following permutations:

$$e = r^3 = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 \end{pmatrix} \quad r = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{pmatrix} \quad r^2 = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 \end{pmatrix}$$

However, there is a more compact notation for these permutations that is even better than what we've used above, and this notation is called *cycle notation*. For example, in *cycle notation* we would write the permutation corresponding to

$r = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{pmatrix}$ as $(1,2,3)$, and as before we usually read this as "1 goes to 2, 2 goes to 3, and 3 goes to 1" event though we really mean "the number currently in position 1 is moved to position 2, the number currently in position 2 is moved to position 3, and the number currently in position 3 is moved to position 1."

In a similar way, we can write the permutation corresponding to $r^2 = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 \end{pmatrix}$ as $(1,3,2)$ in order to say that 1 goes to 3, 3 goes to 2, and 2 goes back to 1. And likewise, we could write the permutation corresponding to $e = r^3 = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 \end{pmatrix}$ as $(1,1)(2,2)(3,3)$ for 1 goes to 1, 2 goes to 2, and 3 goes to 3. However, this looks unnecessarily complicated, and it is more often abbreviated as $(1)(2)(3)$. But we normally don't stop there. We abbreviate it even further! In particular, if we have a permutation like $\begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 3 & 2 \end{pmatrix}$ where 1 goes to 1, 2 goes to 3, and 3 goes to 2, then instead of writing that as $(1)(2,3)$, we usually just shorten that to $(2,3)$. Furthermore, if the permutation is the *identity permutation* which changes nothing, then it is quite common these days to write it simply as $e = (\ )$, a pair of parentheses with nothing inside. Thus, $(1)(2)(3) = e = (\ )$.

MULTIPLYING PERMUTATIONS

Let's suppose that we have just four objects that we'll label 1, 2, 3, and 4, and let's also consider some permutations of these objects. In particular, let's start with $(1,2)$ and $(2,3,4)$. We call the first permutation a *cycle of length 2* or a 2-*cycle* because it moves just two of the objects. It just moves 1 to 2 and 2 back to 1, and because the positions of only two objects are being switched, we also call a 2-*cycle* a *transposition*. On the other hand, $(2,3,4)$ is a *cycle of length 3* or a 3-*cycle* since it moves three objects. Equivalently, we could say that it is a 3-*cycle* since if we keep repeating this *cycle*, then by the third time that we move what is in position 2 to position 3, what's in position 3 to position 4, and what's in position 4 to position 2, we'll be right back where we started! Thus, repeating the *cycle* $(2,3,4)$ three times is equivalent to the identity element, doing no change at all.

At this point you might realize that what we are really talking about is multiplying one permutation by another by simply following one by the other. For example, let's now talk more formally about what we mean by $(1,2)\cdot(2,3,4)$, the product of $(1,2)$ and $(2,3,4)$. The first things you need to know are:

- Some mathematicians do this multiplication from left to right while others do it from right to left.
- Changing which direction you multiply in will often make a difference in the result because multiplication of permutations is generally not *commutative*, i.e. the order in which you multiply the permutations generally makes a difference.
- We'll always multiply from left to right because that is the convention that is followed in some of the useful software tools like GAP (*Groups, Algorithms, and Programming*), and it is also the convention that is generally followed when describing moves for Rubik's cube.

Now, to determine the product $(1,2)\cdot(2,3,4)$, let's revert to our earlier notation, $(1,2)=\begin{pmatrix}1&2&3&4\\ \downarrow&\downarrow&\downarrow&\downarrow\\ 2&1&3&4\end{pmatrix}$ and $(2,3,4)=\begin{pmatrix}1&2&3&4\\ \downarrow&\downarrow&\downarrow&\downarrow\\ 1&3&4&2\end{pmatrix}$. If we do our multiplication by first applying the permutation $\begin{pmatrix}1&2&3&4\\ \downarrow&\downarrow&\downarrow&\downarrow\\ 2&1&3&4\end{pmatrix}$ followed by $\begin{pmatrix}1&2&3&4\\ \downarrow&\downarrow&\downarrow&\downarrow\\ 1&3&4&2\end{pmatrix}$, then we can say that the first permutation sends what's in position 1 to position 2 and the second permutation sends what's in position 2 to position 3. Therefore, in our abbreviated form, we say that 1 goes to 3. Now the question is where does 3 go? Well, the first permutation fixes 3 at 3, but the second permutation sends 3 to 4. Therefore, the end result is that 3 goes to 4. Next, we need to track what happens to 4. The first permutation sends 4 to 4, but the second one sends 4 to 2. Therefore, when the first permutation is followed by the second, 4 goes to 2. And now, we consider the movement of 2. The first permutation sends 2 to 1 while the second sends 1 to 1. Therefore, in the product, 2 goes to 1. Thus, we can now write the product of these permutations as follows:

$$\begin{pmatrix}1&2&3&4\\ \downarrow&\downarrow&\downarrow&\downarrow\\ 2&1&3&4\end{pmatrix}\cdot\begin{pmatrix}1&2&3&4\\ \downarrow&\downarrow&\downarrow&\downarrow\\ 1&3&4&2\end{pmatrix}=\begin{pmatrix}1&2&3&4\\ \downarrow&\downarrow&\downarrow&\downarrow\\ 3&1&4&2\end{pmatrix}$$

In *cycle notation*, though, this would look like:

$$(1,2)\cdot(2,3,4)=(1,3,4,2)$$

Also, it's very easy to figure this out as we go when we write this in cycle notation. For example, consider:

$$(1,2)\cdot(2,3,4)=(1,3,4,2)$$

Going from left to right, we see 1 goes to 2 and then 2 goes to 3, so in the product we have 1 goes to 3:

$$(1,2)\cdot(2,3,4)=(1,3,?)$$

Next, we start with 3, and again doing our permutations from left to right we have that 3 goes to 3 followed by 3 goes to 4, and hence, in the product 3 goes to 4:

$$(1,2)\cdot(2,3,4)=(1,3,4,?)$$

Now we begin again with 4, and we can see that 4 goes to 4 followed by 4 goes to 2, so in the product we have 4 goes to 2:

$$(1,2)\cdot(2,3,4)=(1,3,4,2,?)$$

And lastly, 2 goes to 1 followed by 1 goes to 1, so in the product we have 2 goes to 1:

$$(1,2)\cdot(2,3,4)=(1,3,4,2)$$

And that's it! The product of our 2-*cycle* with a 3-*cycle* results, in this case, in the 4-*cycle* $(1,3,4,2)$. Notice, too, that if we write our multiplication in the opposite order, then we get a different result:

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

We could express our logic for this result in symbolic form by letting $"\rightarrow"$ mean "goes to" and by letting $"\Rightarrow"$ mean "implies." Thus:

$$\begin{aligned}
&2\rightarrow 3 \quad \text{and} \quad 3\rightarrow 3 \quad \Rightarrow \quad 2\rightarrow 3\\
&3\rightarrow 4 \quad \text{and} \quad 4\rightarrow 4 \quad \Rightarrow \quad 3\rightarrow 4\\
&4\rightarrow 2 \quad \text{and} \quad 2\rightarrow 1 \quad \Rightarrow \quad 4\rightarrow 1\\
&1\rightarrow 1 \quad \text{and} \quad 1\rightarrow 2 \quad \Rightarrow \quad 1\rightarrow 3
\end{aligned}$$

There are now several remarks we can make. First, notice that the *cycle* $(2,3,4,1)$ can also be written as $(3,4,1,2)$ or $(4,1,2,3)$ or $(1,2,3,4)$. In other words, it doesn't matter which number or object we put first.

Second, notice that $(2,3,4)(1,2)=(2,3,4,1)\neq(1,3,4,2)=(1,2)(2,3,4)$. Hence, the multiplication is not *commutative*. The order in which we multiply makes a difference.

Third, notice that the *inverse* of $(2,3,4,1)$ is given by just writing this cycle in reverse order as $(1,4,3,2)$.

Lastly, if we have two cycles such as $(1,2)$ and $(3,4)$ which have no elements in common, then these cycles will *commute* with one another. In other words, $(1,2)(3,4) = (3,4)(1,2)$. And furthermore, when two cycles have no elements in common, we say that they are *disjoint cycles*.

And finally, for practice, make sure you now understand how to get each of the following products:

- $(1,2)(1,3) = (1,2,3)$
- $(1,2,3)(3,2,1) = (1)(2)(3) = ( )$
- $(1,2)(3,4,5) = (1,2)(3,4,5) = (3,4,5)(1,2)$

PERMUTATION GROUPS

Let's suppose that we now have just three objects that we'll label 1, 2, and 3, and let's start with the permutations $(1,2)$ and $(1,2,3)$. If, next, we look at all finite products that can be formed from these permutations, then for now take my word that the *set* of all such distinct products will be a *group of permutations of order 6*, or, in other words, a *group* containing 6 elements. We can list those elements as follows:

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

$$(1,2,3)$$

$$(1,3,2) = (1,2,3)^2$$

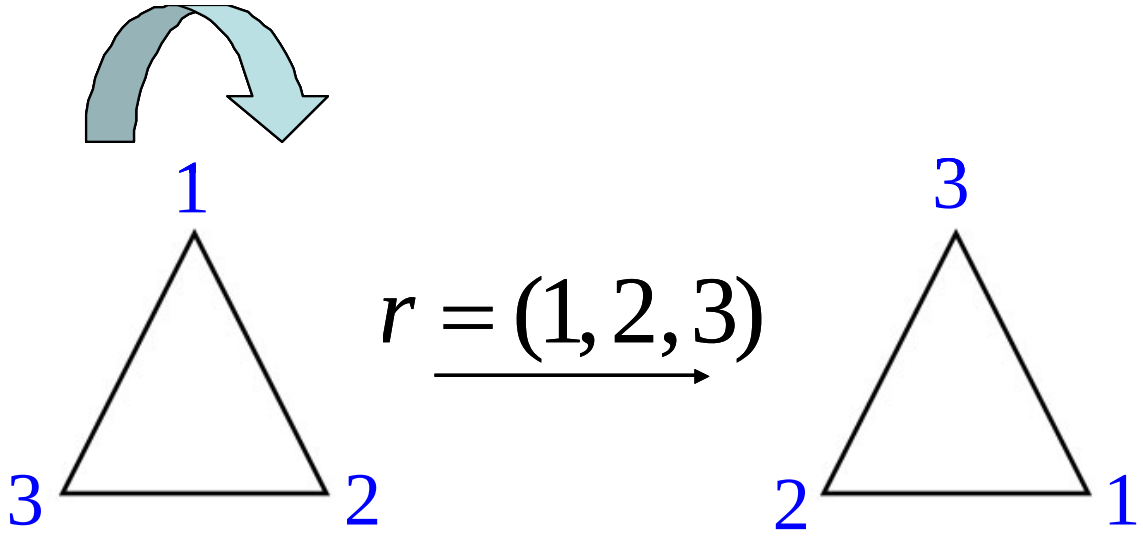
$$(1,2)$$

$$(1,3) = (1,2)(1,2,3)$$

$$(2,3) = (1,2)(1,2,3)^2 = (1,2)(1,3,2)$$

Notice, too, that $(1,2,3)^2$ means $(1,2,3)\cdot(1,2,3)$ while $(1,2,3)^3$ means $(1,2,3)\cdot(1,2,3)\cdot(1,2,3)$. Also, since our *group* can be created by looking at all the distinct finite products we can create by multiplying $(1,2)$ and $(1,2,3)$ together, we call $(1,2)$ and $(1,2,3)$ *generators* of our *group*.

Now let's revisit the multiplication table for the *cyclic group* that resulted from rotating an equilateral triangle clockwise through angles that are *integer* multiples of $120°$.



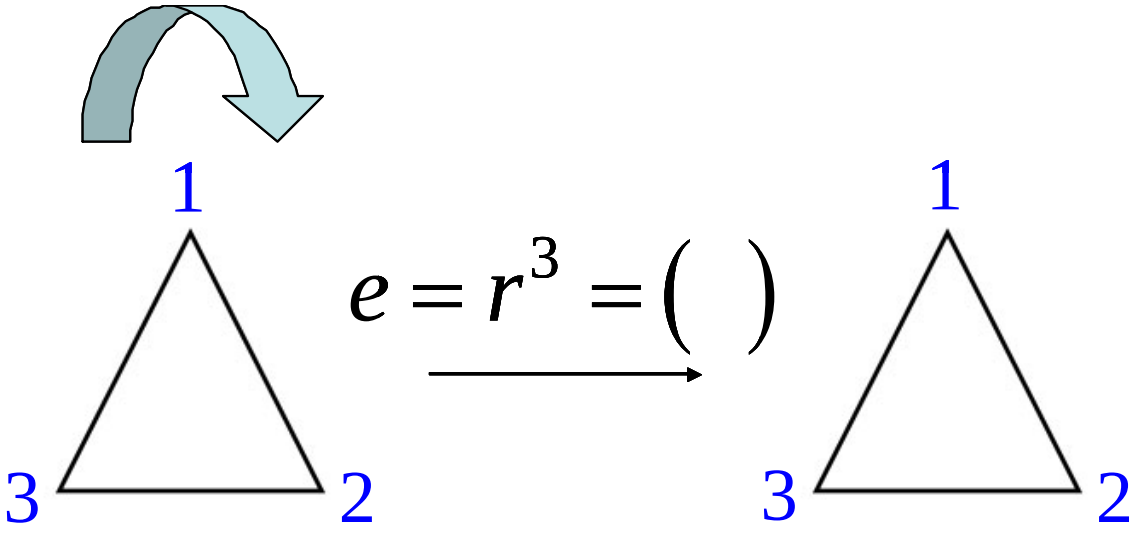
The resulting multiplication table is:

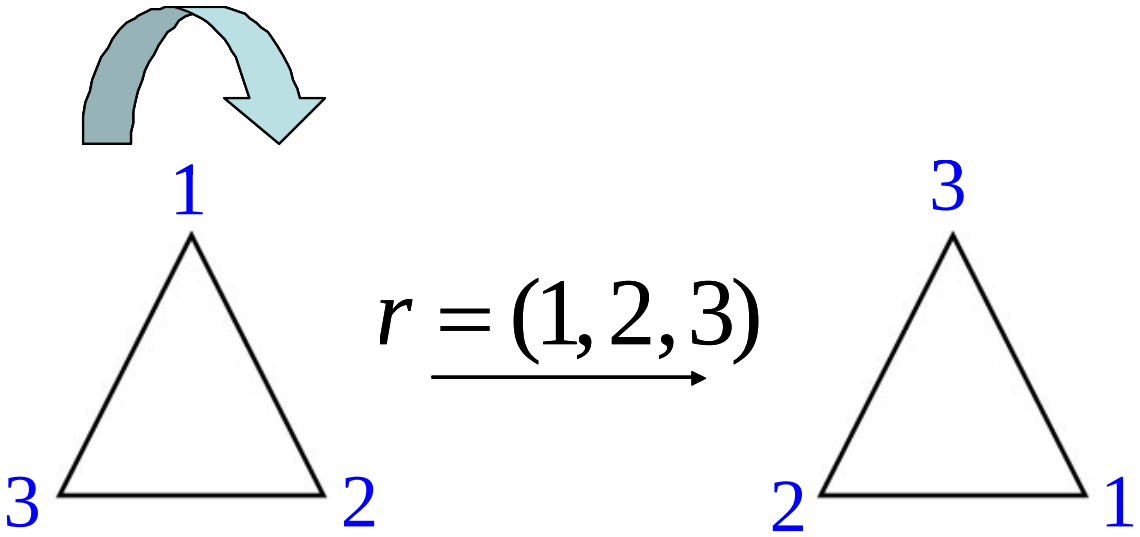
·	e	r	r^2
e	e	r	r^2
r	r	r^2	e
r^2	r^2	e	r

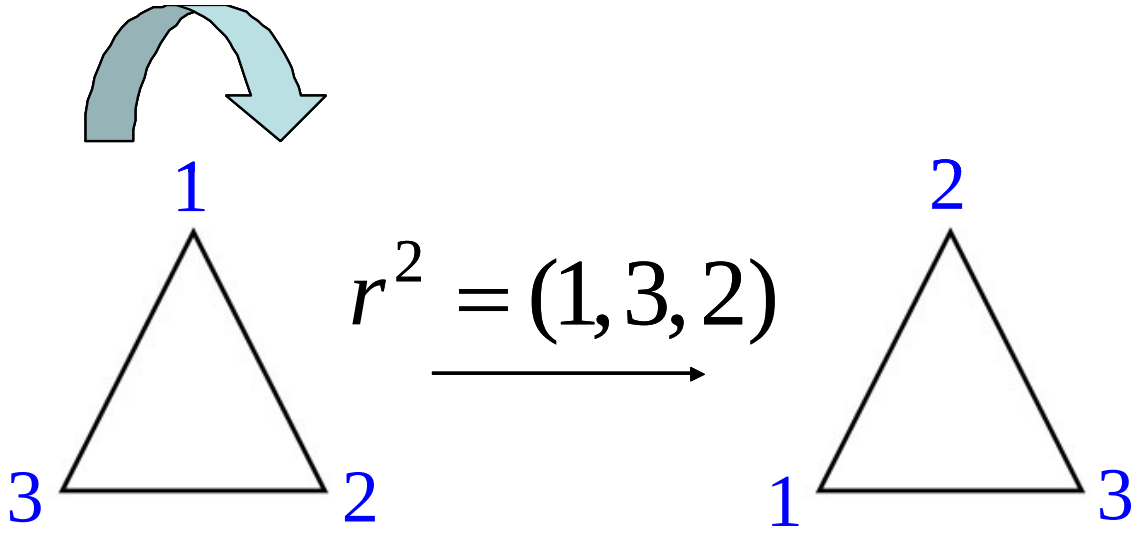
The elements of this *group* are *e*, *r*, and r^2, and notice that each row in our table of products also represents a different permutation of these three elements. We won't do a formal proof at this point, but this should be enough of a clue for you to believe that given any *group*, we can associate each element of that *group* with a permutation of all the elements of that *group*. Hence (and this is very important), every *group* can be represented as a *group* of permutations of some set of objects! We will focus primarily on *finite groups*, and in that case we can say that every finite *group* of *n* elements can be expressed in terms of a *group* of permutations of those *n* elements.

GROUP ACTIONS

Let's now revisit once again our by now very familiar *cyclic group of order 3* that we get when we examine rotations of an equilateral triangle about its center through angles that are *integer* multiples of $120°$. When we did this earlier, we identified the following distinct rotations along with the following multiplication table.







$\cdot$	e	r	r^2
e	e	r	r^2
r	r	r^2	e
r^2	r^2	e	r

However, since our rotations also result in permutations of the numbers, 1, 2, and 3, we can also express our multiplication table in terms of permutations that are written in *cycle* notation. In other words,

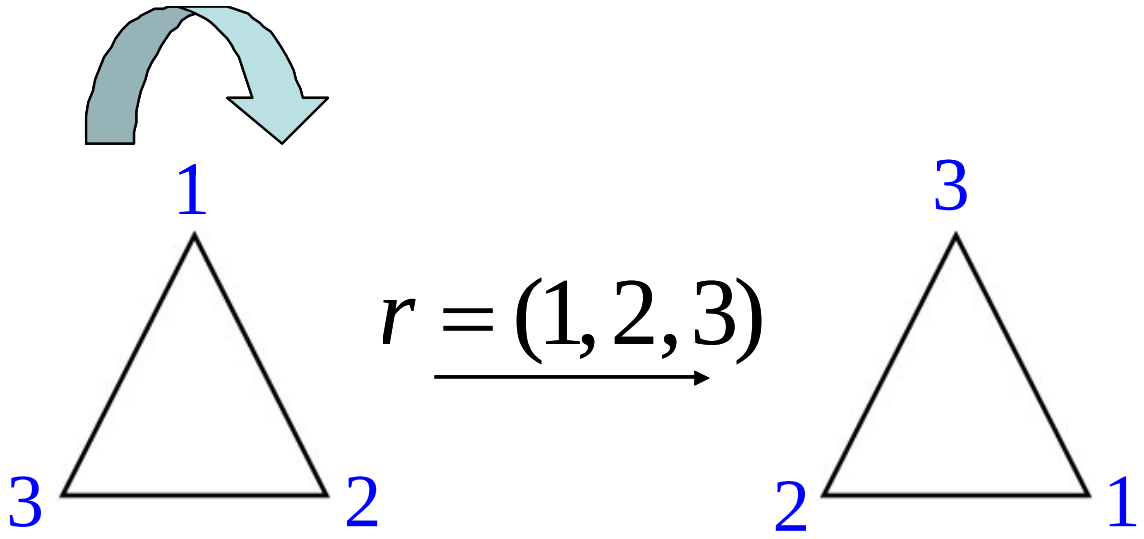
$e = (1)(2)(3) = (\ )$
$r = (1,2,3)$
$r^2 = (1.3.2)$

This, in turn, gives us the following multiplication table:

$\cdot$	$(\ )$	$(1,2,3)$	$(1,3,2)$
$(\ )$	$(\ )$	$(1,2,3)$	$(1,3,2)$
$(1,2,3)$	$(1,2,3)$	$(1,3,2)$	$(\ )$
$(1,3,2)$	$(1,3,2)$	$(\ )$	$(1,2,3)$

Now let's briefly review what is happening here. First, we could say that we have a *set* of objects that we'll designate as $A = \{1,2,3\}$, and then, second, we have a *group* of permutations that we'll call $G = \{(\ ),(1,2,3),(1,3,2)\}$ that interacts with the set *A* by producing different arrangements of the elements in *A*. When this

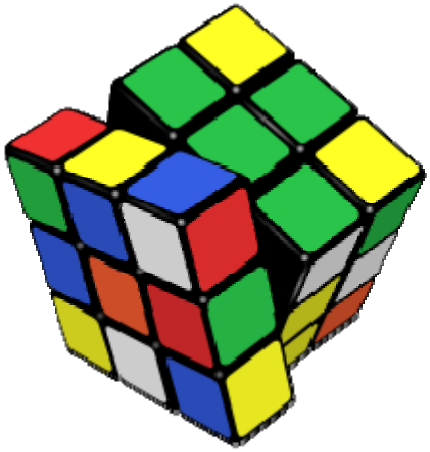
happens, when we have a *group of permutations* that produces different arrangements of the elements of a *set*, we say that the *group* acts upon the set and we call this a *group action*. For example, think of our set $A=\{1,2,3\}$ as our labels for the vertices of an equilateral triangle, and let our *permutation group G* be the *cyclic group* generated by $r=(1,2,3)$, the clockwise rotation of our triangle $120°$ about its center. Then this gives us a very concrete example of a *permutation group* physically acting upon the triangle (or the labels for the vertices of the triangle, if you prefer).



Now this is not an isolated occurrence in *group theory*. It is, in fact, the very norm because recall that given any *group*, we can associate each element of that *group* with a permutation of the *group elements*. Consequently, every *group* can be expressed as a *permutation group*, and every *group element* can be thought of as a permutation that acts upon the very elements of the *group* that it belongs to. The bottom line is that a very natural way to think of all *groups* is in terms of permutations being applied to some *set* of objects. Thus, always ask yourself what the permutations are and what objects are being permuted.

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 called *cubelets*, and then each colored face of a *cubelet* is called a *facelet*. In all, Rubik's cube contains 26 *cublets* and 54 *facelets*. 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 *cubelet*, and 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 face 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 $R2$. Similarly, we'll use R^3 or $3R$ or $R3$ 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 $R4$) 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 *Ri*. 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 realize, the mathematics of permutations has an awful lot to do with helping us understand the structure of Rubik's cube, and, in fact, if we look at all the distinct configurations of the cube that are possible by performing the moves *R, L, U, D, F,* or *B,* then it can been proven that $43,252,003,274,489,856,000$ permutations are possible. Furthermore, the moves *R, L, U, D, F,* and *B* generate a *permutation group* of this size. Also, notice that if we let *A* be the *set* consisting of the 54 *facelets* of Rubik's cube and if we let *G* denote the *group* of $43,252,003,274,489,856,000$ permutations that is generated by the moves *R, L, U, D, F,* and *B*, then Rubik's cube offers us a classic example of a set of objects that is *acted upon by a group*. The *Rubik's cube group* acts upon the cube by creating various permutations of its 54 *facelets*.

Immediately following this brief introduction to Rubik's cube are instructions for solving the cube, and it is highly recommended that you master this solution

because, as we shall see later on, Rubik's cube illustrates in very concrete ways many of the important tools and concepts of *group theory*. Also, 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!*

RUBIK'S® CUBE

THE ULTIMATE BRAIN TEASER

Twist it & turn it to line up the same colors on all sides. Once you solve it, challenge yourself to beat your best time!

Contents: • Rubik's® Cube • Plastic Stand

For 1 Player • AGES 8+

RUBIK'S® CUBE

7-STEP SOLUTION GUIDE

How each step works

B -Twist the Back Face a quarter turn clockwise

Ri - Twist the Right Face a quarter turn counter-clockwise

Example turns

Each step can be used to solve up to FOUR pieces if there are none solved when you start the step. Please note that these illustrations display a sample of a situation on your cube for ONE of the possible FOUR pieces needing to be solved. In many cases, you will need to rotate the cube to a new starting face (with red, orange, yellow or white center square) and repeat the instructions in order to place/rotate all of the pieces in that step before moving on. The end result will only come AFTER all four sides of the cube have been through that step's sequence and all the pieces are in their proper location and oriented properly to match the surrounding center square colors. As such, you may have to repeat the same step a few times with different sides as the starting face until all the pieces are solved.

Step 1

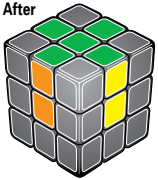
Solve the Upper Green Cross

HINT: To solve the green cross, you have to solve each green edge piece on your own, one-by-one. The tricky part is not messing up the ones you've already solved. First solve the red-green edge, then the white-green edge, then the orange-green edge, then the blue-green edge. You have to figure out this part for yourself. Should you ever have an edge piece in the correct place but flipped the wrong way, use this step to flip it without affecting the other three green edges. Just hold the cube with the piece in the upper-right position as in the picture below, and do the sequence **Ri • U • Fi • Ui**. The edge piece will now be solved, and you can work on the next edge piece.

Before

Ri • U • Fi • Ui

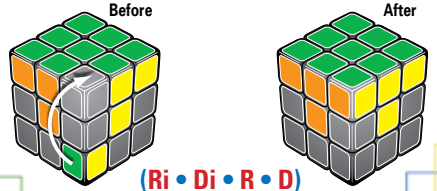
After



Step 2

Solve the Green Corners

HINT: Find a corner piece in the bottom layer that belongs on top. Turn the bottom layer until that piece is directly below its home in the top layer. Hold the cube with the piece at the lower-front-right and its home at the upper-front-right, as in the picture, and then do the sequence **Ri • Di • R • D**, 1, 3, or 5 times until that corner is solved. If you find a corner piece that's already in the top layer but it's in the wrong spot or flipped the wrong way, just hold the cube with that piece in the upper front right position, and do **Ri • Di • R • D** once. Now the piece is in the bottom layer, and you can solve it as described above.

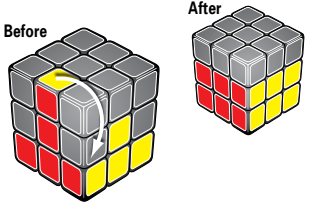


(Ri • Di • R • D)
x 1, 3 or 5

Step 3

Solve the Middle Layer Edges

HINT: Now flip the cube over so green is on the bottom. Try to find the red-yellow edge piece. If it's in the top layer, turn it until the edge matches one of the pictures below. Then do the corresponding sequence to solve it. If the red-yellow edge piece is somewhere in the middle layer, but it's in the wrong place or flipped the wrong way, hold the cube so that the red-yellow edge is in the front-right position, and do either sequence once. (This may require you to rotate the cube to a new face). After the move, the piece is in the top layer, and you can solve it as described above. Repeat this for the other 3 middle-layer edges.



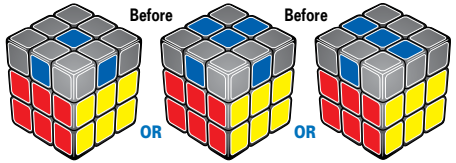
U • R • Ui • Ri
Ui • Fi • U • F

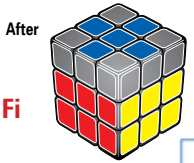
Ui • Fi • U • F
U • R • Ui • Ri

Step 4

Solve the Upper Blue Cross

HINT: Turn the top layer until the edges match one of these pictures. If you do the sequence below once and you still don't have a blue cross, then repeat this step until you do. It doesn't matter which face you start with. Note: In this step, there will be other blue pieces showing on your cube that do not appear in these diagrams.





F • R • U • Ri • Ui • Fi

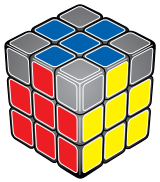
Step 5

Solve the Top Edges

HINT: Hold the cube with red in front. Turn the top layer until the red and blue edge piece is solved as in the picture, and then repeat the sequence below until the yellow and blue edge piece is also solved, on the right side. Now turn the whole cube so that white is the "Front" face. If the top white edge isn't solved, just do the sequence once more, followed by "**U**" to position all the edges properly.

Before

After



R • U • Ri • U • R • U • U • Ri

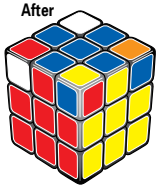
Step 6

Solve the Top Corners

HINT: Find a corner piece that's in the right place, and hold the cube with that piece above your right thumb. In the picture, this piece is the blue, yellow, and red piece. Don't turn the top layer at all, because you will mess up the edges that you just solved in step 5. Now do the sequence below once or twice to put the other 3 corners into the right places. If you can't find a corner piece in the right place, just do the sequence below once before you start this step.

Before

After



U • R • Ui • Li • U • Ri • Ui • L

Step 7

Solve the Top Corners

HINT: Hold the cube with red in front. Keep turning the top layer until the upper-front-right corner needs to be flipped, to have blue on top, like in the picture. Do the sequence below either 2 or 4 times to flip the corner so that blue is on top. Note: As you work through this step, lower layer colors may become scrambled. Don't worry, just keep going! With red still in front, keep turning the top layer and do the sequence again whenever needed to flip the upper-front-right corner piece. When all the corners have been flipped, just turn the layer to solve the cube. Congratulations, you've done it!

Before

OR

After

(Ri • Di • R • D)
x 2 or 4

About your Rubik's Cube

RUBIK'S Cube is just one of a series of exciting puzzles designed to challenge your mind and capture your imagination. With amazing movement of color and pieces, each puzzle offers an intricate challenge that is hard to put down. And just in case it has you stumped, this 7-Step Solution Guide will help you master the challenge.

RUBIK Fact: *RUBIK'S Cube was invented by Erno Rubik, a Hungarian Professor of Architecture and Design. Within one year of its launch in 1980, it became the fastest-selling puzzle the world has ever known. Rubik's Cube is now the best-selling puzzle ever, with over 250 million cubes sold.*

RUBIK Fact: *Most cubes can be solved in only 17 moves with the aid of a computer, and theoretically there is no cube that requires more than 20 twists to solve. Some people can solve the cube in under 45 moves from any scrambled position; and a few can even solve the cube blindfolded!*

The 7-Step Solution Guide

Each step involves a sequence of twists of the cube to move a particular square. To solve the cube, just repeat the steps!

Each face of the cube is assigned a letter (shown below). Each step is made up of a sequence of twists (a one quarter-turn of the face of the cube). To complete the sequence for each step, twist one face of the cube, then twist the next face, and so on, for the complete sequence. The letter 'i' means inverse, or counter-clockwise. Before you start each move, be sure to place your thumbs on the F side of the cube, as shown in the illustration. This will ensure that your cube is properly oriented to execute the move.

Turn clockwise

R - Right Face
L - Left Face
B - Back Face
D - Down Face
F - Front Face
U - Upper Face
?i - Inverse (turn Counter-clockwise)

Important!
To turn a face clockwise, imagine you are facing that side of the cube.

Billions of Combinations, One Solution!

RUBIK'S® Cube is the incredibly addictive, multi-dimensional challenge that has fascinated puzzle fans around the world. Over 250 million cubes have been sold and at least one in every five people in the world has twisted, jumbled and enjoyed this immensely popular puzzle.

RUBIK'S® Cube has been called "the perfect puzzle" and "the best puzzle ever." With a few turns, you mix up its small colored cubes. Now match the cubes back up again to make every side a solid color. You can solve **RUBIK'S® Cube** from any starting point and from any topsy-turvy arrangement of colors. With the right twists, anybody can do it, and with 43 quintillion (43,252,003,274,489,856,000) combinations, no challenge is ever the same!

RUBIK's Facts: 22.95 seconds! That's how long a high school student from Los Angeles took to unscramble the cube and win the Budapest world championship in 1982.

Dan Knights from the USA won the 2003 Rubik's Games Championship held in Toronto, Canada. His average time was just 20 seconds.

The Original Cube is part of an exciting series of puzzles designed to challenge your mind and capture your imagination. Twist and turn the colors & pieces and you'll find an intricate challenge that you won't want to put down.

We will be happy to hear your questions or comments about this game. Please write to: Hasbro Games, Consumer Affairs Dept., P.O. Box 200, Pawtucket, RI 02862 USA. Tel: 888-836-7025 (toll free). European consumers please write to: Hasbro UK Ltd., Hasbro Consumer Affairs, P.O. BOX 43, Caswell Way, Newport, Wales, NP19 4YD, or telephone our helpline on 00 800 2242 7276.

MB GAMES™

Hasbro™

hasbrogames.com

rubiks.com

PROOF OF PURCHASE

MB GAMES™ 16963

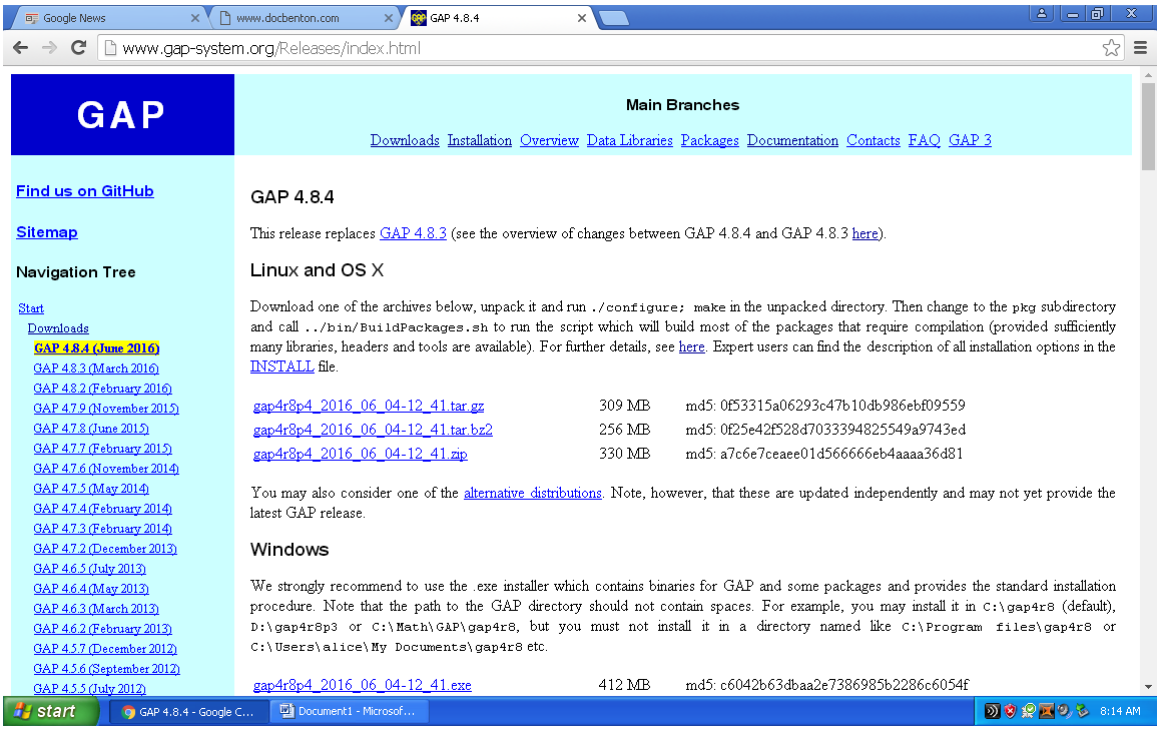
RUBIK'S® CUBE

INSTALLING GAP SOFTWARE

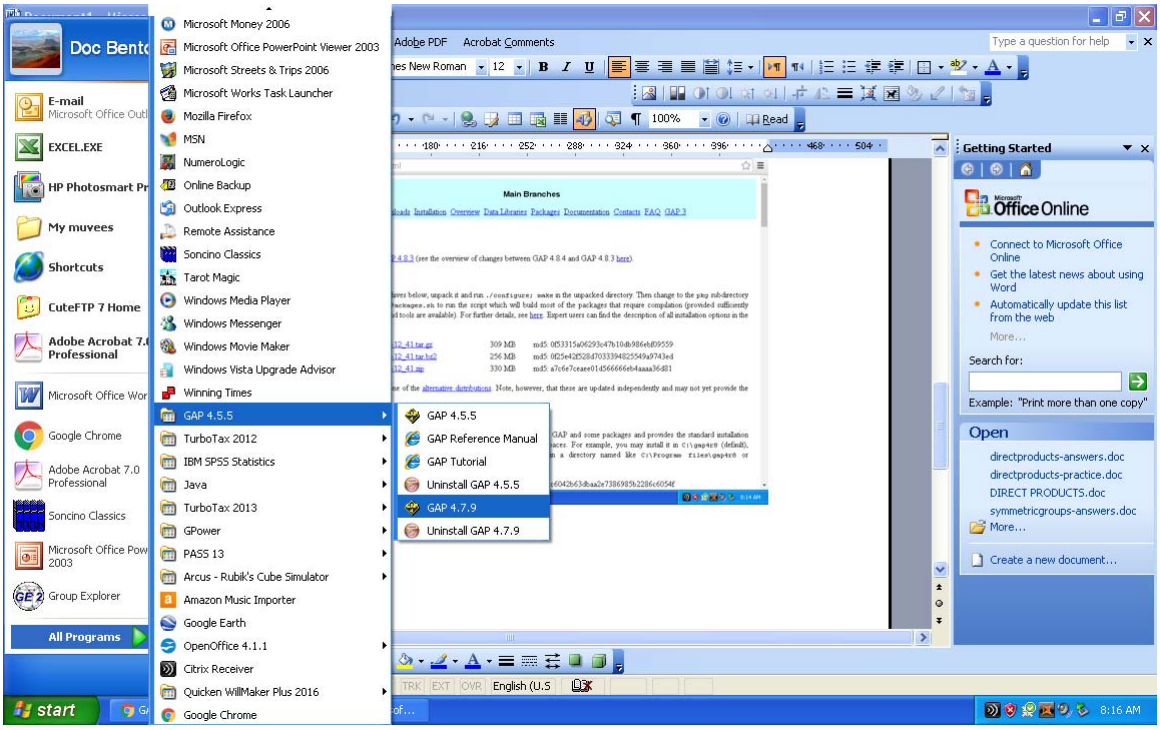
The acronym “GAP” stands for “*Groups, Algorithms, and Programming*,” and it’s a free software program that can be used in the study of *finite groups* as well as other aspects of *abstract algebra*. The best thing about it is that it’s free and it‘s also very useful. The worst thing is that the documentation is not always very clear. Consequently, in the next chapter, “How to Use GAP (Part 1),” I give examples of the coding that must be entered in order to do several of basic things in *group theory* that we’ve talked about so far such as finding the size and the elements of a *group*. In this chapter, though, I just try to show you how to download and install GAP software on a Windows machine.

You can begin by going to http://www.gap-system.org/, and there you will see something similar to the image below..

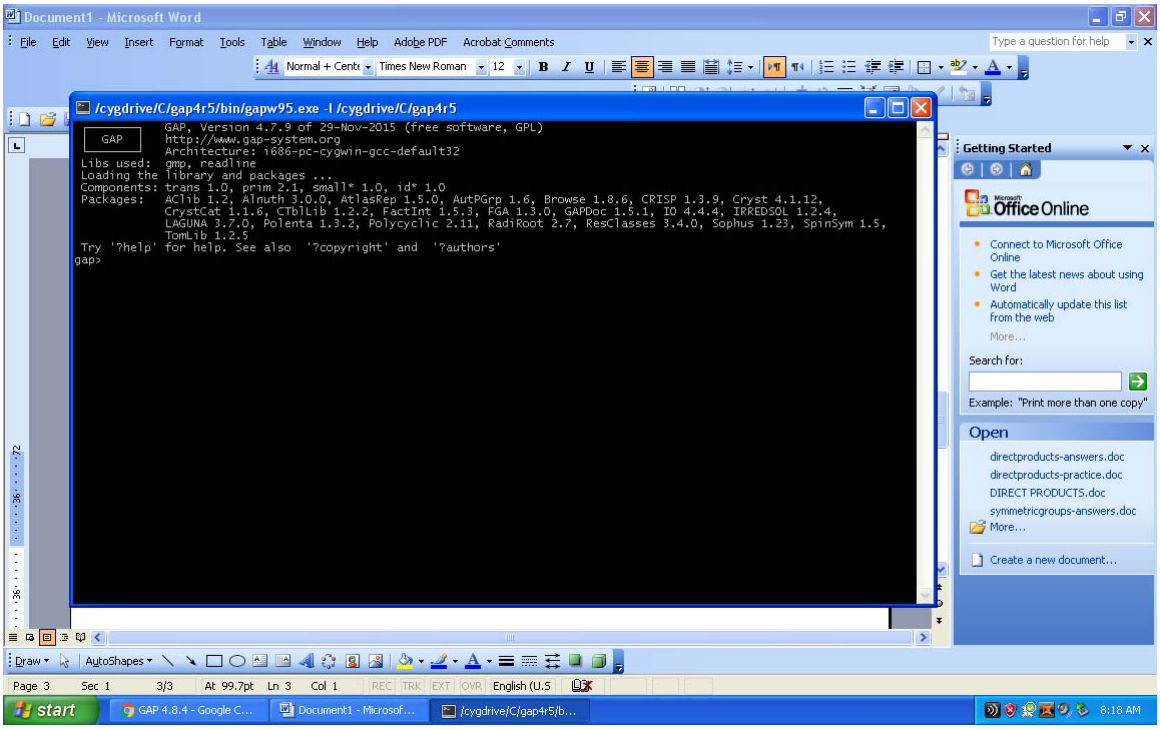
Next, click on the “Downloads” link on the left, find the file that fits your operating system, and once it’s downloaded, double-click on it to install it.



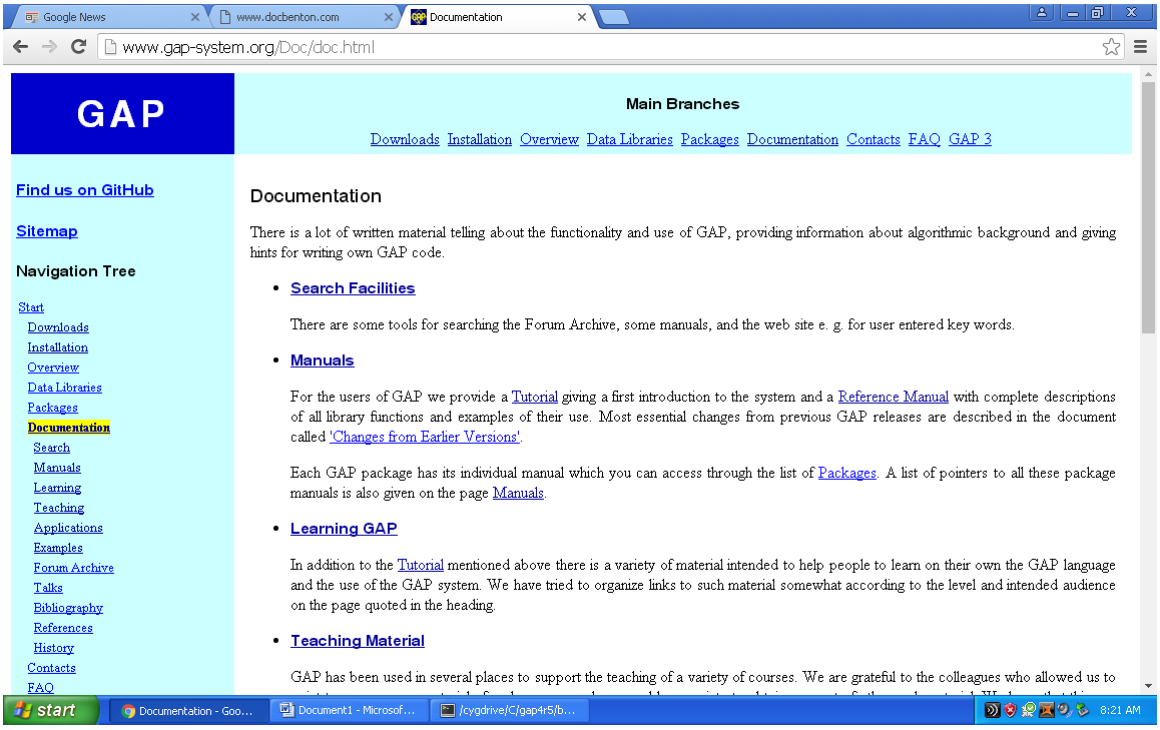
After GAP has been installed, it will appear in your list of programs as follows if you have installed the Windows version.



When you launch the program, it will take a minute or so to load the library and all the subroutine packages. When done, though, this or something similar is what you will see.



The GAP program, as you might expect, is driven by syntax which means that all the commands must be entered in just the right way. For a program like this, I've found that the best way to learn it is to have good examples you can copy and follow, and that's what I present in the chapter "How to Use GAP (Part 1)" that follows this one. There is also online documentation, but it is not always easy to find the examples you need or even to follow the ones you find. To get to the documentation, though, click on the link on the left that says, "Documentation."



From this page, the links to “Tutorial” and “Reference Manual” under “Manuals” are both pretty good. The manual “Abstract Algebra with GAP” is also excellent. And anything else you need to know, you can probably figure out from perusing the webpage for GAP and from doing Internet searches. Enjoy!

And in closing, here is a quick example of me using GAP to find the *group* generated by a couple of permutations and to also find the size of the *group* and the elements of the *group*.

```
gap> a:=(1,2,3);
(1,2,3)
gap> b:=(2,3);
(2,3)
gap> g:=Group(a,b);
Group([ (1,2,3), (2,3) ])
gap> Size(g);
6
gap> Elements(g);
[ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]
gap>
```

HOW TO USE GAP (PART 1)

In my experience, the best way to learn how to use a program like GAP is by learning the commands that help you do those things that you'll probably need or want to do most often. Below is your first set of introductory commands for using GAP software. After launching GAP, I recommend that you type in each command exactly as written and see what happens when you hit the return key. GAP is case-sensitive, and that means that if I've written something below with a capital letter, then you need to also write it with a capital letter. On the other hand, sometimes (but not always!) parentheses can be substituted for brackets. Notice, too, that just about every command ends with a semicolon.

1. *How can I redisplay the previous command in order to edit it?*

   Press down on the control key and then also press p. In other words, "Ctrl p".

2. *If the program gets in a loop and shows you the prompt "brk>" instead of "gap>", how can I exit the loop?*

   Press down on the control key and then also press d. In other words, "Ctrl d".

3. *How can I exit the program?*

   Either click on the "close" box for the window, or type "quit;" and press "Enter."

4. *How do I find the inverse of a permutation?*

```
gap> a:=(1,2,3,4);
(1,2,3,4)
gap> a^-1;
(1,4,3,2)
```

5. *How can I multiply permutations and raise permutations to powers?*

```
gap> (1,2)*(1,2,3);
(1,3)

gap> (1,2,3)^2;
(1,3,2)

gap> (1,2,3)^-1;
(1,3,2)

gap> (1,2,3)^-2;
(1,2,3)

gap> a:=(1,2,3);
(1,2,3)

gap> b:=(1,2);
(1,2)

gap> a*b;
(2,3)
```

```
gap> a^2;
(1,3,2)

gap> a^-2;
(1,2,3)

gap> a^3;
()
gap> a^-3;
()

gap> (a*b)^2;
()

gap> (a*b)^3;
(2,3)
```

6. *How can I create a group from permutations, find the size of the group, and find the elements in the group?*

```
gap> a:=(1,2);
(1,2)

gap> b:=(1,2,3);
(1,2,3)

gap> g1:=Group(a,b);
Group([ (1,2), (1,2,3) ])
```

```
gap> Size(g1);
6

gap> Elements(g1);
[ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]

gap> g2:=Group([(1,2),(1,2,3)]);
Group([ (1,2), (1,2,3) ])

gap> g3:=Group((1,2),(2,3,4));
Group([ (1,2), (2,3,4) ])
```

7. *How can I create a cyclic group of order 3?*

```
gap> a:=(1,2,3);
(1,2,3)

gap> g1:=Group(a);
Group([ (1,2,3) ])

gap> Size(g1);
3

gap> Elements(g1);
[ (), (1,2,3), (1,3,2) ]

gap> g2:=Group((1,2,3));
Group([ (1,2,3) ])
```

```
gap> g3:=CyclicGroup(IsPermGroup,3);
Group([ (1,2,3) ])
```

8. *How can I create a multiplication table for the cyclic group of order 3 that I just created?*

gap> ShowMultiplicationTable(g1);

*	()	(1,2,3)	(1,3,2)
()	()	(1,2,3)	(1,3,2)
(1,2,3)	(1,2,3)	(1,3,2)	()
(1,3,2)	(1,3,2)	()	1,2,3)

9. *How do I determine if a group is abelian?*

gap> g1:=Group((1,2,3));
Group([(1,2,3)])

gap> IsAbelian(g1);
true

gap> g2:=Group((1,2),(1,2,3));
Group([(1,2), (1,2,3)])

gap> IsAbelian(g2);
false

10. *What do I type in order to get help for a command like "Elements?"*

gap> ?Elements

SOMETHING FROM SOMETHING CREATION

We've talked a lot about permutations and *groups* that can be generated by permutations, but now I want to mention an application that is unlikely to be brought up in formal courses on *group theory*. I want to mention *something from something creation*. This is not the type of creation that is preceded by a wonderful "aha" moment. Instead, it is the type of creation where we take what is currently present and just make a different arrangement (permutation) of what already exists. Or, as I say, the only difference between a clean room and a messy room is how things are arranged. One is simply a permutation of the other.

In real life, we tend to engage in *something from something creation* on a daily basis. For example, straightening up your room, washing clothes, or filling a glass with water are all examples of *something from something creation*. In each instance we are taking items that are already present and just creating a different permutation of them. And, again, this is something we tend to do on a daily basis, because without this daily cleanup our environment tends to slip into disarray.

Since *something from something creation* involves permutations, that means that we are also talking about *groups of permutations* such as those we encounter in *group theory*. In a sense, our daily world is an expanded version of Rubik's cube, and we should be trying to find those permutations of reality that make it better for everyone. Thus, for now, we are making the following points:

- *Something from something creation* involves just creating a different arrangement of what's already present in your life.
- The collection of all possible permutations of your environment is a *permutation group*.
- If you want to change your life, move some things around!

SUMMARY (PART 1)

On the one hand, we've covered a lot of material about *group theory* that is likely entirely new to you, but on the other hand, we've barely scratched the surface! Much more is yet to come. Nonetheless, at this point you want to be familiar with the following items:

- The algebraic definition of a *group*.
- *Clock arithmetic* and the *integers modulo n*.
- *Cyclic groups*.
- Symmetry and *group theory*.
- Permutations and *group theory*.
- Any *group* may be expressed as a *group of permutations*.
- A multiplication table for a *group*.
- *Groups acting on a set of objects*.
- Rubik's cube.
- GAP software.
- Our lives are full of cycles.
- Our lives are full of symmetry.
- We can engage in *something from something creation* and change our lives for the better by forming better permutations of what already exists!

PRACTICE (PART 1)

Below are a few things you should do before moving on to Part 2, and they are important because they will help solidify and give you hands-on experience with the things we've been talking about.

1. *Write down from memory the mathematical definition of a group. Construct your own explanation of what each part of the definition means.*

2. *Each one of the examples below fails to be a group. For each given example, identify at least one part of the definition of a group that fails to apply.*

   The integers under subtraction. $(\mathbb{Z}, -)$.

   The integers under division, $(\mathbb{Z}, \div)$.

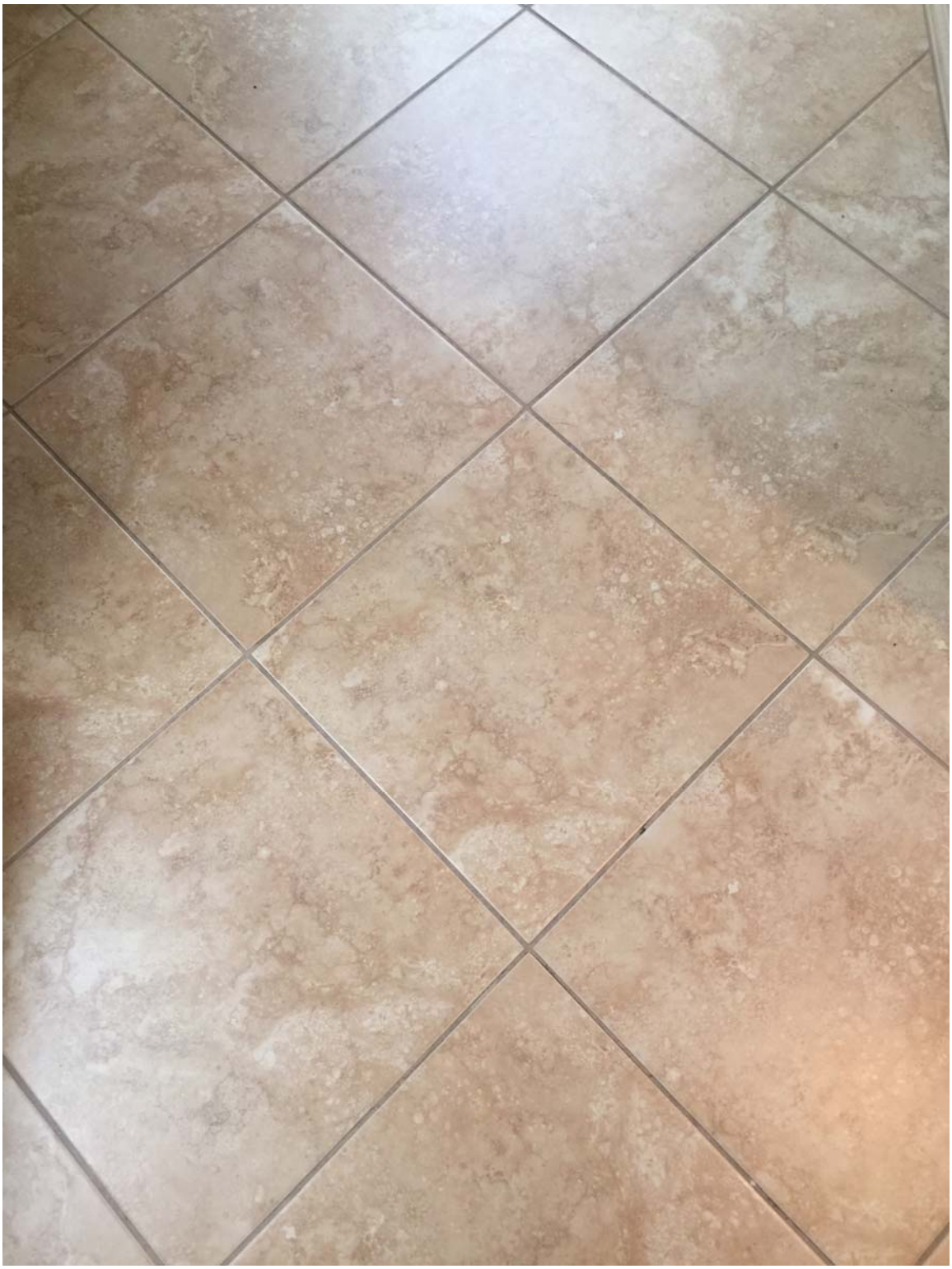
   The real numbers under multiplication, $(\mathbb{R}, \cdot)$.

   The positive real numbers under division, $\left(\mathbb{R}^+, \div\right)$.

3. *Using addition modulo 4, write down an addition table for* $\mathbb{Z}_4$.

4. *Identify as many patterns as possible in the pictures below. What cyclic groups would you associate with any of these patterns? What symmetry do you notice in your own place of residence or work? Answers will vary. (NOTE: At this point we've focused primarily on cycles and cyclic groups, and we can rightly say that every group is built up from cycles and their interactions. However, in Part 2 we will discover other types of groups*

besides the cyclic groups.)



5. *What are some of the repetitive cycles that you go through on a daily or weekly basis?*

6. *How many different permutations can you make of the letters a,b,c? How many different permutations can you make of the letters a,b,c,d?*

7. *Using the instructions included in this document, solve Rubik's cube.*

8. *Perform the calculations below first by hand and then check your results using GAP software.*

   (1,2)(1,3) = ?

   (1,2)(3,4) = ?

   $(1,2,3,4)^2 = ?$

   $[(1,2)(1,3)]^{-1} = ?$

   $(1,2)^{-1} = ?$

9. *Using GAP software, find the group generated by (1,2) and (1,3), find its size, list its elements, and generate its multiplication table.*

10. *Give recent examples of ways in which you have engaged in something from something creation. In other words, list ways in which you have created different permutations of your current reality.*

PRACTICE (PART 1) – ANSWERS

Below are a few things you should do before moving on to Part 2, and they are important because they will help solidify and give you hands-on experience with the things we've been talking about.

1. *Write down from memory the mathematical definition of a group. Construct your own explanation of what each part of the definition means.*

   A group is a nonempty set G along with a binary operation that satisfies the following conditions:

   (Closure) For any two elements a and b in G, we have that ab is an element of G.

   (Associativity) For any three elements a, b, and c in G, we have that (ab)c = a(bc).

   (Identity) There exists an element e in G such that for any element a in G we have that ae = a = ea.

   (Inverses) For any element a in G, there exists an element a^{-1} such that $aa^{-1} = e = a^{-1}a$.

   If the following property also holds, then we call G an abelian or commutative group:

   (Commutativity) For any a and b in G, ab = ba.

2. *Each one of the examples below fails to be a group. For each given example, identify at least one part of the definition of a group that fails to apply.*

The integers under subtraction. $(\mathbb{Z}, -)$.

The associative law fails since (8-4)-2 = 4-2 = 2 while 8-(4-2) = 8-2 = 6. Additionally, there is no identity element. For example, if 8-e=8, then we should have e=0. But since 0-(8) = -8 instead of 8, 0 doesn't work as an identity. Also, if there is no identity, then we can't even talk about inverses.

The integers under division, $(\mathbb{Z}, \div)$.

The associative law fails since (8/4)/2 = 2/2 = 1 while 8/(4/2) = 8/2 = 4. Also, closure fails since ½ is not an integer. Similarly, even though 1 functions as an identity element, an integer like 2 does not have a multiplicative inverse that is an integer whose product with 2 results in 1.

The real numbers under multiplication, $(\mathbb{R}, \cdot)$.

Closure and associativity hold true and the number 1 functions as an identity element, but the number 0 has no multiplicative inverse that you can multiply 0 by in order to get 1.

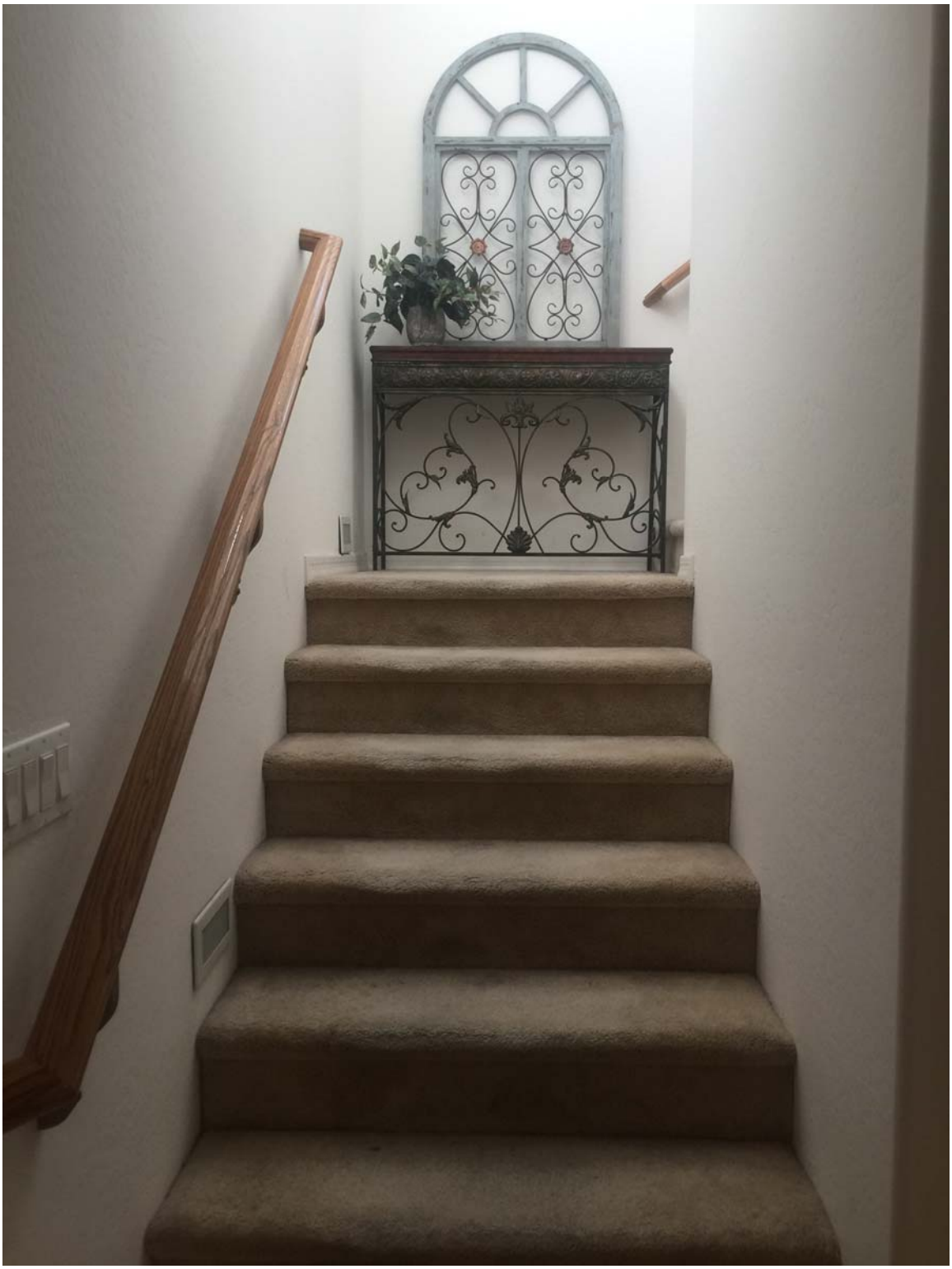
The positive real numbers under division, $(\mathbb{R}^+, \div)$.

The associative law fails since (8/4)/2 = 2/2 = 1 while 8/(4/2) = 8/2 = 4. However, closure, identity, and inverse properties do appear to be satisfied.

3. *Using addition modulo 4, write down an addition table for* $\mathbb{Z}_4$.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

4. *Identify as many patterns as possible in the pictures below. What cyclic groups would you associate with any of these patterns? What symmetry do you notice in your own place of residence or work? Answers will vary. (NOTE: At this point we've focused primarily on cycles and cyclic groups, and we can rightly say that every group is built up from cycles and their interactions. However, in Part 2 we will discover other types of groups besides the cyclic groups.)*



There seem to be 5 identical steps on the stairs in the picture. This symmetry suggests a cyclic group of order 5.

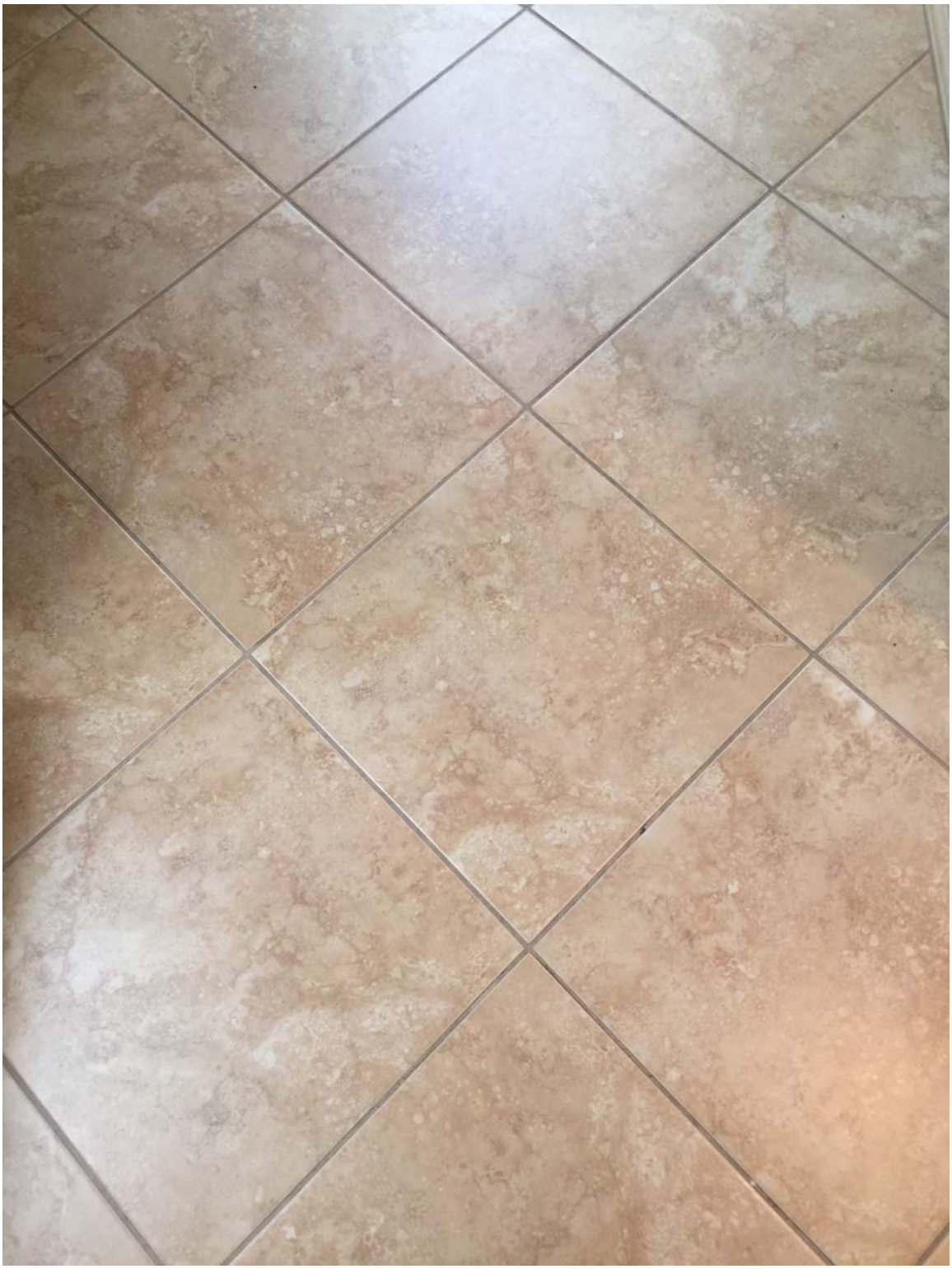
There are 4 identical light switches on the wall at the bottom of the stairs. This symmetry suggests a cyclic group of order 4.

Each light switch can be switched on or off. If we let our operation be a flip, then one flip turns it on while two flips takes us back to where we started. This symmetry suggests a cyclic group of order 2.

The design under the table at the top of the stairs can be reflected across a vertical axis of symmetry. This symmetry suggests a cyclic group of order 2.

The design in the rectangular part above the table contains a piece that can be reflected about both vertical and horizontal axes in order to create the entire design. Each separate reflection by itself suggests a cyclic group of order 2. In Part 2 of this book, however, we will discover other types of groups that can incorporate both reflections into a single group. For now, though, we'll only focus on cyclic groups.

And within the semicircle at the top we see 4 identical "pizza slices." This symmetry suggests a cyclic group of order 4.



In the tile design above we could take a single square and move it from west to east or from south to north or along a diagonal from southwest to northeast or along a diagonal from northwest to southeast. If we take any of these directions and imagine the tiles extending to infinity, then a single square tile can generate what we call an infinite cyclic group that is isomorphic to the integers. For example, no movement corresponds to 0 while movement by 2 squares in one direction corresponds to 2 and movement by 2 squares in the opposite direction corresponds to -2.

Additionally, each square can be rotated about its center through angles that are multiples of $90°$ in order to generate a cyclic group of order 4. Or, you could think of taking a single side of a single square and moving it from, for example, left side to top side to right side to bottom side and then back to left side. This symmetry also suggests a cyclic group of order 4.

Each individual leaf has bilateral symmetry that suggests a cyclic group of order 2. The elements of this group consist of either doing nothing at all (the identity) or doing a flip about the axis of symmetry. However, in addition to the bilateral symmetry of a single leaf, one may glide each leaf a bit along a stem and then reflect it across the stem. This results in what is called a "glide reflection."

5. *What are some of the repetitive cycles that you go through on a daily or weekly basis?*

   A cycle that I repeat fairly regularly is to wake up, drink coffee, work, eat lunch, nap, eat dinner, watch TV with my wife, sleep, and then repeat. This activity defines a cyclic group of order 8.

6. *How many different permutations can you make of the letters a,b,c? How many different permutations can you make of the letters a,b,c,d?*

   Six permutations. Also, we can derive this result by realizing that if we are constructing a particular permutation, then we have 3 choices for the first letter, 2 for the second, and 1 for the last letter. This means that the total number of permutations we can construct is (3)(2)(1)=6.

abc	bac	cab
acb	bca	cba

   Twenty-four permutations. Also, we can derive this result by realizing that if we are constructing a particular permutation, then we have 4 choices for the first letter, 3 choices for the second letter, 2 for the third letter, and 1 for the last letter. This means that the total number of permutations we can construct is (4)(3)(2)(1)=24.

abcd	bacd	cbad	dbca
abdc	badc	cbda	dbac
acbd	bcad	cabd	dcba
acdb	bcda	cadb	dcab
adbc	bdac	cdba	dabc
adcb	bdca	cdca	dacb

7. *Using the instructions included in this document, solve Rubik's cube.*

   Done!

8. *Perform the calculations below first by hand and then check using GAP software.*

   $(1,2)(1,3) = (1,2,3)$

```
gap> (1,2)*(1,3);
(1,2,3)
```

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

```
gap> (1,2)*(3,4);
(1,2)(3,4)
```

   $(1,2,3,4)^2 = (1,2,3,4)(1,2,3,4) = (1,3)(2,4)$

```
gap> (1,2,3,4)^2;
(1,3)(2,4)
```

   $[(1,2)(1,3)]^{-1} = (1,2,3)^{-1} = (3,2,1) = (1,3,2)$

```
gap> ((1,2)*(1,3))^-1;
(1,3,2)
```

   $(1,2)^{-1} = (1,2) = (2,1)$

```
gap> (1,2)^-1;
(1,2)
```

9. *Using GAP software, find the group generated by (1,2) and (1,3), find its size, list its elements, and generate its multiplication table.*

```
gap> a:=(1,2);
(1,2)

gap> b:=(1,3);
(1,3)

gap> g:=Group(a,b);
Group([ (1,2), (1,3) ])
```

```
gap> Size(g);
6

gap> Elements(g);
[ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]

gap> ShowMultiplicationTable(g);
*       | ()      (2,3)   (1,2)   (1,2,3) (1,3,2) (1,3)
--------+-----------------------------------------------
()      | ()      (2,3)   (1,2)   (1,2,3) (1,3,2) (1,3)
(2,3)   | (2,3)   ()      (1,2,3) (1,2)   (1,3)   (1,3,2)
(1,2)   | (1,2)   (1,3,2) ()      (1,3)   (2,3)   (1,2,3)
(1,2,3) | (1,2,3) (1,3)   (2,3)   (1,3,2) ()      (1,2)
(1,3,2) | (1,3,2) (1,2)   (1,3)   ()      (1,2,3) (2,3)
(1,3)   | (1,3)   (1,2,3) (1,3,2) (2,3)   (1,2)   ()
```

10. *Give recent examples of ways in which you have engaged in something from something creation. In other words, list ways in which you have created different permutations of your current reality.*

I combined hot water and coffee in a cup and drank it.

I moved the trash from the kitchen to the garbage can.

I put on some clothes.

I cleaned up my office.

I pulled some weeds in the backyard.

Study Group Theory. Be a God!