Permutation Groups

Tom Davis
tomrdavis@earthlink.net
http://www.geometer.org/mathcircles
April 2, 2003

Abstract

This paper describes permutations (rearrangements of objects): how to combine them, and how to construct complex permutations from simpler ones. We'll talk a bit about groups of permutations as well. Some interesting examples here are related to solving the "Rubik's Cube" puzzle. It may help have a Rubik's Cube with you as you read along (and a screwdriver to take it apart if you don't know how to solve it).

1 Permutations

A permutation is a rearrangement of objects. Here we will only consider permutations of a finite number of objects, and since the object names don't really matter, we will often simply consider permutations of the numbers $1, 2, 3, \ldots, n$. When we work with Rubik's Cube, however, there are better names for the faces than integers—see Section 3.

Of course we'll learn about permutations first by looking at permutations of small numbers of items, but if you think of the 54 colored faces of the little cubelets ("cubies") on Rubik's Cube, you can see that every time you twist a side of the cube, you are rearranging those little faces.

There are plenty of other examples of permutations, many of which are extremely important and practical. For example, when you have a list of items to sort, either by hand or with a computer program, you are essentially faced with the problem of finding a permutation of the objects that will put them in order after the permutation.

If we consider permutations of n objects, there are $n!$ of them. To see this, first consider where object number 1 winds up. There are n possibilities for that. After the fate of object 1 is determined, there are only $n - 1$ possible fates for object number 2. Thus there are $n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1 = n!$ permutations of a set of n objects.

For example, if we consider all possible rearrangements of the set $\{1, 2, 3\}$, there are $3! = 3 \cdot 2 \cdot 1 = 6$ of them, listed in Table 1.

1	$1 \to 1$	$2 \to 2$	$3 \to 3$
2	$1 \to 2$	$2 \to 1$	$3 \to 3$
3	$1 \to 3$	$2 \to 2$	$3 \to 1$
4	$1 \to 1$	$2 \to 3$	$3 \to 2$
5	$1 \to 2$	$2 \to 3$	$3 \to 1$
6	$1 \to 3$	$2 \to 1$	$3 \to 2$

Table 1: Permutations of 3 objects

A good way to think of permutations is this (using permutations of three objects as an example): Imagine that there are three boxes labeled "1", "2", and "3", and initially, each contains a ball labeled with the same number—box 1 contains ball 1, and so on. A permutation is a rearrangement of the balls but in such a way that when you're done there is still only a single ball in each box.

In the table above, the notation $a \to b$ indicates that whatever was in box a moves to the box labeled b, so to apply permutation number 3 above means to take whatever ball is in box 1 and move it to box 3, to leave the contents of box 2 alone, and to take the ball from box 3 and put it into box 1. In other words, permutation number 3 above tells us to swap the contents of boxes 1 and 3.

The notation above is pretty clumsy. Here are a couple of other possibilities:

1.1 Two Row Notation

Write the permutation like this:

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

where the example above indicates that the contents of box 1 moves to box 4, box 2 is unchanged, the ball in box 3 moves to box 1, and the ball in box 4 moves to box 3.

The advantage to this notation is that it is very easy to figure out where everything goes. The disadvantage is that it requires writing down each number twice. Since the top row can always be put in order, however, there is no real need to write it, so simply listing the second row is sufficient (assuming there is an obvious way to put the boxes in order). But there is another way that is often far more useful.

1.2 Cycle Notation

Write the example above like this:

$$(143)$$

This indicates that the contents of box 1 moves to box 4, the contents of box 4 to box 3, and the contents of box 3 moves back into box 1. The system is called "cycle notation" since the contents of the boxes in parentheses move in a cycle: 1 to 4, 4 to 3, and 3 back to 1.

Some permutations have more than one cycle. For example, the cycle notation for the permutation corresponding to:

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

is

$$(13)(24).$$

There are two "cycles". 1 moves to 3 and 3 moves back to 1. At the same time, 2 moves to 4, and 4 back to 2. In other words, the contents of boxes 1 and 3 are cycled, and at the same time, the contents of boxes 2 and 4 are cycled.

In cycle notation, there cannot be any duplicate elements in the various cycles that make up the permutation, so something like $(13)(12)$ is not a valid form. As we will see in the next section, something like $(13)(12)$ can be reduced to a valid form—in this particular case to (132).

As a final example, consider this permutation of $\{1, 2, 3, 4, 5, 6, 7, 8\}$:

$$(135)(2768).$$

It moves the ball in box 1 to box 3, 3 to 5, and 5 back to 1. At the same time, it moves 2 to 7, 7 to 6, 6 to 8, and 8 back to 1. Notice that 4 is not involved, so it stays fixed. If you want to make it clear that 4 is a member of the set of items under consideration, but that in this particular permutation it is not moved, you can write:

$$(135)(2768)(4).$$

In fact, the special permutation that does not move anything is often written as: (1).

Note also that the ordering doesn't matter as long as each item to be permuted appears only once, and that you can list a cycle beginning with any member of it. All of the following indicate exactly the same permutation:

$$\begin{array}{lll} (135)(2768) & (2768)(135) & (7682)(135) \\ (351)(6827) & (8276)(513) & (6827)(513) \end{array}$$

Since there are so many possible ways to label a particular permutation, if there is no convention about the labeling, it may be difficult to tell if two permutations are the same or different as the example above illustrates.

If it is easy to assign an order to the elements being permuted as in the example above, then it is best to choose the representation of a permutation as follows, where we assume they elements are $1, 2, 3, \ldots, n$:

1. Begin with the smallest element. If it is moved, list the permutation beginning with that smallest element as the first entry in the cycle.
2. After listing the complete cycle, check to see if there are other elements moved by the permutation that do not appear in the cycle. If so, choose the smallest remaining, and repeat the process until all moved elements are listed.

In the example above, this "canonical" representation would be the first one listed: $(135)(2768)$.

In the rest of this document, we'll use the cycle notation and unless there is a good reason to do otherwise, we will list permutations using their canonical representations.

2 Combining Permutations

Of course it's nice to have a method to write down a permutation, but things begin to get interesting when we combine them. If you twist one face of Rubik's Cube and then twist another one, each twist jumbles the faces, and the combination of two twists usually causes a jumbling that is more complicated than either of the two individual twists.

Rather than begin with Rubik's Cube, let's begin by looking at permutations of just 3 objects. We listed them in Table 1, but there we used a very clumsy notation. Here are the six possible permutations of three items listed in the same order as in Table 1:

$$(1), (12), (13), (23), (123), (132).$$

What happens if we begin with ball 1 in box 1, ball 2 in box 2, and ball 3 in box 3, and then we apply (12) followed by (13)?

A good way to think about this is to follow the contents of the boxes one at a time. For example, ball 1 begins in box 1, but after (12) it has moved to box 2. The second permutation, (13), does not move the contents of box 2, so after both permutations have been applied, ball 1 will have moved to box 2. So the final result will look like this:

$$(12\cdots$$

where we're not sure what comes next. We don't know if 2 will go back to one and the cycle will close, or whether it will continue to another box. So since the fate of 2 is in question, let's see where it goes.

The first permutation, (12) moves box 2 to box 1, and then (13) will move box 1 to box 3, so now we know the combination of permutations looks like this:

$$(123\cdots$$

Since there are only three objects, we know that 3 will go back to 1 and close the cycle, but (especially when you're beginning), it's good to trace each ball, including ball 3 in this case.

The first permutation, (12), does not move the contents of box 3, but the second, (13) moves it to box 1, so the combination of (12) followed by (13) is equivalent to the single permutation (123).

Combining permutations as above is written just like a multiplication in algebra, and we can write our result as follows[1]:

$$(12)(13) = (123).$$

[1] In other places, sometimes this "multiplication" of permutations is written in the opposite order: $(13)(12) = (123)$. There are good reasons to choose either ordering, but here we'll write them in the order they occur from left to right, so $(12)(13)$ means that first (12) is applied, followed by (13).

Beware, however. This is *not* the same as multiplication that you're used to for real numbers. By doing the same analysis as above, convince yourself that:

$$(13)(12) = (132) \neq (123) = (12)(13).$$

In other words, the order of multiplication makes a difference. If P_1 and P_2 are two different permutations, it may not be true that $P_1P_2 = P_2P_1$. Multiplication of permutations is not commutative.

Test your understanding of multiplication of permutations by verifying all of the entries in the "multiplication table" for the permutations of three objects in Table 2.

	(1)	(12)	(13)	(23)	(123)	(132)
(1)	(1)	(12)	(13)	(23)	(123)	(132)
(12)	(12)	(1)	(132)	(123)	(23)	(13)
(13)	(13)	(123)	(1)	(132)	(12)	(23)
(23)	(23)	(132)	(123)	(1)	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	(1)
(132)	(132)	(23)	(12)	(13)	(1)	(123)

Table 2: Multiplication table of permutations

Remember that the order of multiplication is important. In Table 2, if you are trying to look up the product of $(12)(13)$, find the column labeled (12) and the row labeled (13). If you use the row labeled (12) and the column labeled (13) you will be looking up the product $(13)(12)$ which may be different.

As a final check on your understanding of multiplication of permutations, verify the following multiplications of permutations:

$$\begin{aligned} (1342)(3645)(1623) &= (126435) \\ (12)(23)(34)(45) &= (15432) \\ (135)(32)(54321)(413)(13) &= (1) \end{aligned}$$

Here are some general properties of multiplication of permutations. They hold for the sets of permutations of any number of elements, but you should check to see that they do hold in the particular case of the three-element permutations in Table 2.

- **Closure:** If P and Q are two permutations, then the products PQ and QP both make sense in that the result is also a permutation. This is obviously true since a rearrangement of a rearrangement is itself a rearrangement.
- **Identity:** The permutation (1) that leaves everything fixed is an identity under multiplication. If P is any permutation, then $P(1) = (1)P = P$. In other words, the permutation (1) behaves for permutation multiplication just like the number 1 behaves for multiplication of real numbers. Sometimes the identity is written as e. It is not hard to prove that the identity is unique.
- **Inverses:** Every permutation has an inverse that "undoes" the operation. In other words, if you apply a permutation to a set and then apply its inverse, the result is that the final order is unchanged from the original. If P is a permutation and P^{-1} is its inverse, we can write $PP^{-1} = P^{-1}P = (1) = e$.

  If you have a permutation written in cycle notation and you want to find its inverse, simply reverse all the cycles. For example, $[(134)(256)]^{-1} = (652)(431)$. To see why this works, multiply: $(134)(256)(652)(431)$. The result will be (1)[2].

[2]Notice that we have reversed not only the contents of each cycle, but also the order of the cycles. For cycles in the canonical form, reversing the order of cycles is not important, but if the permutation is not in canonical form, reversing both orders will produce the inverse, no matter what.

- **Associativity:** If P, Q, and R are any three permutations, then $P[QR] = [PQ]R$. In other words, if you have to multiply 3 or more permutations together, it doesn't matter how you group them to do the multiplications. We use braces "[" and "]" to indicate the grouping since we've used parentheses to indicate the cycles of the permutations.

  For example, let's work out $(1345)(243)(163)$ two different ways. First we'll multiply (1345) by (243) and then take that result and multiply it by (163). Then we'll do the multiplication beginning with the last two permutations (check these yourself):

$$\begin{aligned}[(1345)(243)](163) &= (1245)(163) = (124563)\\ (1345)[(243)(163)] &= (1345)(16324) = (124563)\end{aligned}$$

- **Not (necessarily) Commutativity:** This is really just a reminder that the commutative law does not hold in general. If you swap the order of a product, the result may change, so PQ and QP are not necessarily the same.

  There are some cases, however, where things do commute. For example, if your permutations are two cycles that share no elements in common, the order in which they occur does not matter. So $(123)(45) = (45)(123)$. This is obviously true since each cycle rearranges a different subset of elements, so their operations are completely independent and can be reversed in order with no effect on the final outcome.

2.1 Powers of Cycles

Because the associative law holds, it makes sense to write something like P^n where P is a permutation and n is a positive integer. $P^4 = PPPP$, and because the operation of permutation multiplication is associative, you get the same answer no matter how you choose to multiply them together.

For example, let's compute P^3, where $P = (134)(25)$.

$$P^3 = PPP = (134)(25)(134)(25)(134)(25) = (25).$$

In fact, it's easy to see how powers work on cycles. Let's look at $P = (123456)$, for example. Here are the various powers of P:

$$\begin{array}{ccc} P^1 = (123456) & P^2 = (135)(246) & P^3 = (14)(25)(36)\\ P^4 = (153)(264) & P^5 = (165432) & P^6 = (1)\end{array}$$

When raising a cycle to a power k, each elements "steps forward" by k steps, cycling back to the beginning, if necessary. It's just like modular (clock) arithmetic. Clearly if the cycle P is n items long, then $P^n = (1) = e$.

It's a great exercise to calculate P^k for all powers of k, where P is a cycle whose length is a prime number. Try it with $P = (1234567)$ and calculate P^1, P^2, P^3, P^4, P^5, P^6, and P^7.

If a permutation is written in proper cycle form where there is possibly more than one cycle, but there are no items that appear in more than one cycle, then taking powers of such a permutation is easy—just raise the individual cycles to the power and combine the results. This is because individual cycles that do not share items do commute, so, for example,

$$[(123)(45)]^3 = (123)(45)(123)(45)(123)(45),$$

but the (123) and the (45) cycles commute, so the right hand side can be rearranged to be:

$$\begin{aligned}[(123)(45)]^3 &= (123)(123)(123)(45)(45)(45)\\ &= (123)^3(45)^3.\end{aligned}$$

Clearly, if P is a cycle of length n, then $P^n = e$ because each application of the cycle moves all the elements in the cycle one step forward. For any permutation, we say that the order of the permutation is the smallest power of that

permutation that is the identity. Thus if P is a cycle of 17 elements, it will have order 17, since 17 applications of it will return every ball to its original box.

If P is not a cycle, but is written in proper cycle form, then the order of P is the least common multiple of the cycle lengths. This is pretty obvious—consider the permutation $P = (12345)(678)$. If we consider that $P^n = (12345)^n(678)^n$, then to make $P^n = e$, we must have that both $(12345)^n = e$ and $(678)^n = e$. The first will be true if n is a multiple of 5; the second if n is a multiple of 3. For both to be true, n must be a multiple of both 5 and 3, and the smallest number that is both is the least common multiple of the two: 15 in this case.

3 The "Befuddler" Notation

From now we will use Rubik's Cube for some of our examples of permutations. For that reason, we need a reasonable notation to describe the moves that can be made. Here we are talking only about the standard $3 \times 3 \times 3$ cube, although much of what we do can easily be applied to other versions.

The cube has six faces, each of a different color, but different cubes have different coloring patterns, so it is useful to have a notation that is independent of the particular coloring of a cube.

Here is a good method to describe a general move. Imagine that you hold the cube in front of you looking directly at the center of one face, and with the top and bottom faces parallel to the ground. There are six faces—the front and back, the up and down, and the left and right. Conveniently, the first letters of these words are all different: F, B, U, D, L, R. Rearrange them as "$BFUDLR$", and it reminds you of the English word, "befuddler", which is also appropriate for describing the general difficulty of the problems presented by the cube.

There are six primitive moves that can be made—any of the six faces can be turned 1/4 turn clockwise. Obviously, if you want to turn a face counter-clockwise, that's what you would do, but to keep the description mathematically simple using the minimum number of primitive operations, remember that a single twist counter-clockwise is the same as three clockwise twists.

By "clockwise" is meant that if the face in question is grasped in the right hand, it is turned in the direction pointed to by the right thumb.

We will use the befuddler letters as names for these primitive moves. Thus the move "F" means that the front face is turned 1/4 turn clockwise, et cetera. We can combine letters as well. "FUB" means first twist the front face clockwise, then twist the up face, then the back face. All twists are 1/4 turn clockwise. To turn the front face by 1/2 turn or 3/4 turn (3/4 turn clockwise = 1/4 turn counter-clockwise), use the notation F^2 or F^3. Note that $F^4 = B^4 = U^4 = D^4 = L^4 = R^4 = e$, so we could write F^3 as F^{-1} equally well. We will tend to use the F^{-1} form here.

As a final example, F^2U^3TBD means to turn the front face a half turn, then twist the up face 1/4 turn counter-clockwise, followed by a 1/4 clockwise twist of the top, then back, and then down faces.

If you think of the entire cube as being composed of a bunch of smaller "cubies", the befuddler notation gives a good method to name the individual cubies. The cubies in the corners are identified by the three faces they share. The cube on the up right front can be called URF, and so on. The edge cubies are identified by the two faces it lies on, so the one on the up and front faces would be called UF. But in order to distinguish between the cubie UF and the transformation that is a rotation about the up face followed by a rotation about the front face, we will put boxes around the cubie names: $\boxed{URF}$ and $\boxed{UF}$ for the cubes just mentioned.

With this cubie notation, we can describe (using our permutation cycle notation) certain results that transformations may achieve. For example, ($\boxed{LD}$ $\boxed{FD}$ $\boxed{RD}$) refers to an operation that cycles the left-down, front-down, and right-down cubies. The left-down cubie moves into front-down postion, et cetera.

The notation still isn't perfect. You'll find that when you solve Rubik's cube that sometimes a cubie will be in the right place in the cube, but rotated (if it's a corner cubie) or flipped (if it's an edge cubie). But we can describe it as follows. Suppose there is an operation that leaves everything fixed, but flips $\boxed{UB}$ and $\boxed{UL}$ in place. We can write this as: $\boxed{UB}$, $\boxed{UL} \rightarrow \boxed{BU}$, $\boxed{LU}$.

4 Groups and Subgroups

A group is a system consisting of a set of objects and a binary operation that produces from any two objects another object that satisfies the conditions listed in Section 2 (having an identity, an inverse, and with an associative operation). The set of all possible permutations of a set of elements is a special group called the "symmetric group". The symmetric group on n objects is the group consisting of all permutations of n elements, so it contains $n!$ elements—in other words, the symmetric groups get big pretty fast as n gets larger. In this paper we will denote the symmetric group on n elements by S_n.

Most practical applications use only a subset of the possible permutations. In Rubik's Cube, for example, although there are 54 little colored faces, it is clear that the ones in the corners will always be in some corner, the ones on the edges remain on the edges, and the ones in the centers of the faces remain centers of faces. Thus in the collection of permutations reachable from a solved cube, there are none that move, say, a corner to an edge.

We will be interested in special subsets of groups that are themselves groups—in other words, a non-empty subset of the permutations so that any product of permutations in the subset is another permutation in the subset.

In our earlier example of S_n (the symmetric group on three elements), there are the following subgroups (including the group that contains only the identity and the entire symmetric group):

$$\{(1)\},\ \{(1),(12)\},\ \{(1),(13)\},\ \{(1),(23)\},\ \{(1),(123),(132)\},$$
$$\{(1),(12),(13),(23),(123),(132)\}.$$

There aren't any others. If you try to construct some, you'll see what happens. As an example, suppose we try to make one that contains (12) and (123).

It will have to contain $(12)^2 = (1)$ and $(123)^2 = (132)$. It will also have to contain $(123)(12) = (23)$ and $(132)(12) = (13)$. But now we've shown that it must contain all the permutations in the symmetric group, so S_3 is the group generated by (12) and (123).

If you are a beginner with Rubik's Cube and you want to practice with some operations that jumble the cube but do not jumble it into a nightmare, consider restricting yourself to a subgroup of all the allowable moves. Here are a couple of good examples:

- Only allow moves that consist of 180° turns of two opposite faces at the same time. Basically, there are only 3 moves: R^2L^2, U^2D^2, and F^2B^2. These generate some nice patterns as well. This is a very simple subgroup.
- This one is more complicated, but still not too bad. It's basically the same as the one above, except that you're allowed to do single turns of the opposite faces, such as LR^{-1}, UD^{-1}, and FB^{-1}. By repeating these moves you can, of course, get to any position in the subgroup above, but there are *many* more possibilities.

5 Even and Odd Permutations

Begin with the following exercise: verify the following products of permutations:

$$\begin{aligned}(12) &= (12)\\ (12)(13) &= (123)\\ (12)(13)(14) &= (1234)\\ (12)(13)(14)(15) &= (12345)\end{aligned}$$

Although the expressions on the left are not in proper cycle notation, this does show that any cycle can be expressed as a product of 2-cycles, or exchanges. This example shows that a cycle of n objects can be written as a product of $(n-1)$ 2-cycles.

In fact, there are clearly an infinite number of ways to express any permutation as a product of 2-cycles:

$$(123) = (12)(13) = (12)(13)(12)(12) = (12)(13)(12)(12)(12)(12) = \cdots$$

But it is true that if a permutation can be written as an even number of cycles, any representation will contain an even number of cycles. In the example above, (123) was expressed as $2, 4, 6, \cdots$ cycles. Similarly, if a permutation allows a representation as an odd number of cycles, all its 2-cycle representations will contain an odd number of 2-cycles. All permutations can be divided into these "even" and "odd" permutations.

It requires proof, of course, that it is impossible to represent a permutation with both an even and an odd number of 2-cycles, and that will be shown in Section 5.1.

The identity is an even permutation (zero 2-cycles), and clearly if you multiply any even permutation by another even permutation, you will get an even permutation. Thus the set of all permutations that are even form a subset of the full symmetric group. This is called the "alternating group", and the alternating group on n objects is called A_n.

Table 3 is the multiplication table for the alternating group A_4. It is a great example of a group that is complicated, but not too complicated. See what subgroups of it you can find.

	(1)	(123)	(124)	(134)	(234)	(132)	(142)	(143)	(243)	(12)(34)	(13)(24)	(14)(23)
(1)	(1)	(123)	(124)	(134)	(234)	(132)	(142)	(143)	(243)	(12)(34)	(13)(24)	(14)(23)
(123)	(123)	(132)	(13)(24)	(234)	(12)(34)	(1)	(143)	(14)(23)	(124)	(134)	(243)	(142)
(124)	(124)	(14)(23)	(142)	(13)(24)	(123)	(134)	(1)	(243)	(12)(34)	(143)	(132)	(234)
(134)	(134)	(124)	(12)(34)	(143)	(13)(24)	(14)(23)	(234)	(1)	(132)	(123)	(142)	(243)
(234)	(234)	(13)(24)	(134)	(14)(23)	(243)	(142)	(12)(34)	(123)	(1)	(132)	(143)	(124)
(132)	(132)	(1)	(243)	(12)(34)	(134)	(123)	(14)(23)	(142)	(13)(24)	(234)	(124)	(143)
(142)	(142)	(234)	(1)	(132)	(14)(23)	(13)(24)	(124)	(12)(34)	(143)	(243)	(134)	(123)
(143)	(143)	(12)(34)	(123)	(1)	(142)	(243)	(13)(24)	(134)	(14)(23)	(124)	(234)	(132)
(243)	(243)	(143)	(14)(23)	(124)	(1)	(12)(34)	(132)	(13)(24)	(234)	(142)	(123)	(134)
(12)(34)	(12)(34)	(243)	(234)	(142)	(124)	(143)	(134)	(132)	(123)	(1)	(14)(23)	(13)(24)
(13)(24)	(13)(24)	(142)	(143)	(243)	(132)	(234)	(123)	(124)	(134)	(14)(23)	(1)	(12)(34)
(14)(23)	(14)(23)	(134)	(132)	(123)	(143)	(124)	(243)	(234)	(142)	(13)(24)	(12)(34)	(1)

Table 3: The Alternating Group A_4

5.1 Parity Preservation

Earlier in this section we showed that it is possible to represent any permutation as a product of 2-cycles, and we stated without proof that any such representation of a given permutation will always contain an even number of cycles or it will always contain an odd number of cycles. We will prove that fact by showing that it is possible to assign a parity (even or odd) to any permutation in a unique way and that multiplication of an even permutation by a 2-cycle produces an odd permutation and vice-versa.

When written in canonical form, a permutation will have a certain number c_1 of 1-cycles, c_2 of 2-cycles, c_3 of 3-cycles and so on. We define the parity of such a permutation as:

$$\sum_n c_n(n+1) \mod 2. \tag{1}$$

This makes sense from the observation that $(123\cdots n) = (12)(13)\cdots(1n)$ so every cycle of length n can be written as a product of $n-1$ different 2-cycles. What we will show is that if this permutation is multiplied by another 2-cycle that the parity of the sum in equation 1 switches.

Assume that every element is listed in the canonical permutation representation including those elements that do not move which are listed as 1-cycles. If this permutation is multiplied by the 2-cycle (km) then there are two possibilities: either the two elements k and m are in the same cycle or they appear in different cycles (where the cycles in which they appear may have length 1).

First consider the case where they lie in the same cycle. That cycle will look like this: $(kk_2k_3 \cdots k_i m m_2 \cdots m_j)$. This cycle contains $i+j$ elements and will thus add $i+j+1$ to the sum in equation 1. If this cycle is multiplied on the right by (km), we obtain: $(kk_2 \cdots k_i)(mm_2 \cdots m_j)$. The two resulting cycles of lengths i and j will add $i+1+j+1$ to the sum, so the parity will switch.

Finally, if k and m appear in different cycles: $(kk_2k_3 \cdots k_i)(mm_2 \cdots m_j)$, then if this is multiplied on the right by (km) we obtain: $(kk_2 \cdots k_i m m_2 \cdots m_j)$. In this case, the original cycle form contributed $i+1+j+1$ to the sum in equation 1 and after multiplication the single cycle result contributes $i+j+1$, so again, the parity changes.

5.2 The 4×4 Sliding Block Puzzle

You have probably seen the sliding block puzzle with 4×4 spaces and 15 blocks numbered 1 through 15, and the object is to try to slide them until they are in order. If you begin will all of them in order except that 14 and 15 are reversed, there is no solution. In other words, there is no way to convert the situation shown below on the left to the "solved" condition on the right.

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

This can be proved by showing that the sliding operation is like a permutation group, and that the swapping of two blocks amounts to an odd permutation in that group, but the operation of sliding a block is an even permutation. No matter how many even permutations you put together, it will never be odd.

A	B	C	D
E		F	G
H	I	J	K
L	M	N	O

A	B	C	D
E	F	G	K
H	I	J	O
L	M	N	

A	B	C	D
E	I	F	G
H	J	K	O
L	M	N	

The basic idea is illustrated in the diagrams above. Suppose that initially the situation is as shown in the left-most diagram where the variables A through N represent the numbers 1 through 15 in some order. For any such situation where the open square is not in the lower-right corner, we agree to convert it to that form first by moving all possible blocks to the left and then moving all possible blocks up. The result of this when applied to the left diagram is the diagram in the center. After these moves are made, the situation is a pure permutation of the numbers 1 through 15 which has either even or odd parity.

On the left, there are four possible moves. If E or F is moved, then the situation is unchanged after moving the blank square to the lower-right as described above. But if block I is moved up then after the movement of the blank square to the lower-right corner is shown in the diagram on the right. It is easy to check that this is obtained from the one in the middle by the permutation $(FIJKG)$–an even permutation. Thus in both cases, the result of a movement of a single block results in an even permutation of the blocks. Obviously a few other cases need to be considered, but the results will be similar. Hence, it is impossible to reverse just one pair of blocks such as swapping the 14 and 15 pair.

6 Generators

Suppose you pick some complete symmetry group and choose some number of permutations from it. Then you construct the smallest subgroup that contains all of them. This is the subgroup generated by the initial set of permutations you chose.

Using again S_3 as our example, what is the subgroup generated by $\{(123)\}$? Well, it has to contain (123) itself, $(123)^2 = (132)$, $(123)^3 = (1)$ and nothing else since higher powers of (123) start repeating: $(123)^4 = (123)^3(123) = (1)(123) = (123)$. In general, if $n >= 3$, $(123)^n = (123)^{n-3}$. We know that $\{(1),\ (123),\ (132)\}$ is a subgroup of S_3 so it is the subgroup generated by (123).

Using Rubik's Cube as an example, if you've played with it, you know that there are billions (acutally, there are a lot more!) of permutations in the "Rubik's Cube group", but if we consider as a generator a 1/4-twist of the front (in other words, the F move), you can see that if that is the only operation you're allowed to do, there are only four possible rearrangments of the cube you can achieve. So that particular generator will generate a subgroup of size 4.

If you have a cube handy, here's an exercise. Begin with a solved cube. You are only allowed to make two sorts of move: F^2 and R^2, in other words, only 180° rotations about the front and right faces are allowed. These moves certainly are permutations of the cube's faces. Show that the order of the subgroup they generate is 6. In other words, show that you can only get the cube into 6 different patterns (including the "solved" pattern) if F^2 and R^2 are the only allowed moves.

If we have a finite group (and that's the only sort we consider in this paper), every element has some finite order. The proof is easy:

Let P be some permutation, and consider $P^1, P^2, P^3, \ldots$. eventually, since there are only a finite number of elements in the group, there has to be some i and j such that $P^i = P^j$. Assume $j > i$. Then $P^{j-i}P^i = P^j = P^i$. Thus $P^{j-i} = e$, the identity.

We can also see that it's true since every permutation expressed in proper cycle form will have an order equal to the least common multiple of the lengths of its cycles as we stated previously. The advantage of the proof in the previous paragraph is that it applies to all finite groups—not just permutation groups.

On the other hand, it is sometimes quite difficult to guess what the order of an element of the permutation group might be. For example, consider the following permutation of Rubik's Cube: FR. Suppose that it is one indivisible move. it is obvious that both the F and R moves by themselves have order 4—4 such turns return the cube to the original condition. But if you consider the pair of turns to be a single move, what is the order of that? The answer turns out to be 105—not an obvious result!

My initial (and very painful) solution to the cube was based on the above concept. I knew that any operation, if repeated enough times, would return an initially solved cube back to the solved condition. But by experimentation, I found that if my operation required, say, 24 repeats to get from solved to solved, very often the condition after 12 or 8 moves (these are divisors of 24) would leave most of the cubies fixed.

It is pretty obvious why this works. Imagine a permutation with a cycle structure like this: $P = (123)(4567)(89)$. We know that $P^{12} = e$, but what does P^6 or P^4 look like? Work it out: $P^6 = (46)(57)$, $P^4 = (123)$. Do you see what's going on?

Here is an interesting exercise. Show that if you have a subgroup of S_n that contains (12) and $(123\cdots n)$, then the subgroup is the entire group S_n. In other words, any possible permutation of n objects can be expressed as some product of a 2-cycle and an n-cycle. (Hint: If $P = (123\cdots n)$, consider the permutations $P(12)P^{-1}$, $P^2(12)P^{-2}$, $\ldots$, $P^n(12)P^{-n}$.)

7 Conjugates

If P and Q are any permutations, then the permutation PQP^{-1} is called a conjugate of P. In group theory, a conjugate operation is very much like a change in coordinate system.

Here's a concrete example from Rubik's Cube. Suppose that you know how to swap two corner pieces that are on the same edge (see Section 10.1; let's call this operation Q), but you're faced with a cube where the corners you would like to swap are not on the same edge. No problem—find a simple operation (call it P) that brings the two corners of interest to be on the same edge. If you perform P, then Q, and then "undo" P (in other words, perform P^{-1}, the net effect will be to move the corners to the same edge, swap the corners on that edge, and then move the corners back to where they began. Doing P, then Q, then P^{-1} is the same as doing PQP^{-1}—a conjugate of Q.

8 Commutators

If P and Q are any permutations, then the commutator of P and Q is $PQP^{-1}Q^{-1}$. It's just a conjugate with one additional operation of Q^{-1} tagged onto the end.

Here's an example of a commutator in action. Suppose that you want to find an operation that flips two edge cubies on the same face in place without affecting any of the other cubies. It's not hard to find a series of moves that leaves one face completely fixed except for flipping a single cubie on it but perhaps hopelessly jumbles the rest of the cube. Call the operation that does this P. Now let Q be a single twist of that face that puts another cubie in the same slot where the flipped cubie was. What does $PQP^{-1}Q^{-1}$ do?

P flips the cubie (but trashes the rest of the cube that's not on the face). Q moves a different cubie to that slot. P^{-1} then undoes all of the damage caused by P on the rest of the cube, but flips the new cubie. Q^{-1} just rotates the face in question back to its original condition. The operation in Section 10.4 is just such a commutator.

9 Representations of Arbitrary Groups

In Section 4 we stated that groups are usually defined without reference to permutations. The mathematical definition of a group is simply a set of elements and a binary operation on that set that has an identity, inverses of each element, and is associative. In fact, the "multiplication table" listed below represents a valid binary operation on the elements $E, A, B,$ and C where E is the identity:

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

It is easy to prove, however, that for any such group it is possible to define a permutation group that behaves in *exactly* the same way. Here is how to do it for the group above: $E \leftrightarrow (e)(a)(b)(c)$, $A \leftrightarrow (ea)(bc)$, $B \leftrightarrow (eb)(ac)$ and $C \leftrightarrow (ec)(ab)$. Do you see how this is related to the group multiplication table?

Check to see that the operations work the same. For example, show that if $AB = C$, then the product of the permutations corresponding to A and B yield the permutation that corresponds to C, et cetera.

Thus, in a sense, *all* groups can be considered to be permutation groups.

10 Interesting Rubik Permutations (Spoiler!)

This section contains enough information for you to solve your cube without much thinking. Don't look at it if you like to solve puzzles by yourself.

Here are some operations that may prove to be useful in solving the cube puzzle. The first three move the cubies as indicated, but some of them also may flip the edges or rotate the corners. The final two operations leave all the cubies in place, but flip edge cubies or rotate corner cubies as indicated.

There are almost certainly better methods available—these are just the ones I found myself. For the initial stages of solving a cube, they are also too powerful. If you're just trying to get the top face correct from a completely jumbled cube, you don't really care what you do to the other cubies, but all the examples below are very restrictive—*only* the indicated cubies move; the others are left fixed by the operations.

Warning: If you're starting with a pure cube, be careful to follow the instructions below exactly—one error and your cube will be trashed. Take it slowly and remember that B is "back", not "bottom". Also remember that to undo an operation, you can reverse the steps starting from the back. For example, to reverse $FL^{-1}D^2RUR^{-1}$, perform $RU^{-1}R^{-1}D^2LF^{-1}$. Also, be sure to keep the top cube on top and the right cube on the right as you do these operations. For example, if the top cube is white when you begin, make sure it stays white through all the operations. Another way to avoid problems when you are a beginner is always to twist the faces with your right hand. Then if it is one of F, B, L, R, U, or D, you will twist in the direction of your thumb. If the operation is among F^{-1}, B^{-1}, L^{-1}, R^{-1}, U^{-1}, or D^{-1}, you'll twist away from your thumb. If you're left-handed, think different.

Finally, it is much easier to study movements if you can begin with a solved cube, but it's pretty easy to make an error and to wind up with a cube that's totally jumbled. If you have no idea how to solve it, this situation can be pretty depressing. But there is a way to cheat— just take the cube apart, and put it back together in the solved configuration. To take the cube apart, the easiest way is to take a screwdriver and to put it between the center cubie of a face and one of the edge cubies, and then to pry out the edge cubie. Once it's out, it is easy to remove all the rest of the cubies, leaving a central "skeleton". From the skeleton, put the cubies back one at a time into their correct positions.

10.1 Swap Two Corners

This operation swaps two corners, but also jumbles some edge cubies. Use it if you're planning to get the corners in place first, and then work on the edges. In addition to the permutation specified, it also twists $\boxed{LFD}$.
($\boxed{RBD}$ $\boxed{LBD}$)($\boxed{RB}$ $\boxed{FD}$ $\boxed{BD}$ $\boxed{LD}$): $RD^{-1}R^{-1}D^{-1}B^{-1}DB$.

10.2 Cycle Three Edge Cubies

($\boxed{LD}$ $\boxed{FD}$ $\boxed{RD}$): $R^{-1}LBRL^{-1}D^2R^{-1}LBRL^{-1}$.
($\boxed{UF}$ $\boxed{UB}$ $\boxed{DB}$): $R^{-1}LU^2RL^{-1}B^2$.

10.3 Cycle Three Corner Cubies

($\boxed{LUF}$ $\boxed{RUB}$ $\boxed{LUB}$): $URU^{-1}L^{-1}UR^{-1}U^{-1}L$.

10.4 Flip $\boxed{UB}$ and $\boxed{UL}$ In Place

$\boxed{UB}$, $\boxed{UL}$ → $\boxed{BU}$, $\boxed{LU}$: $R^{-1}LB^2RL^{-1}D^{-1}R^{-1}LBRL^{-1}ULR^{-1}B^{-1}L^{-1}RDLR^{-1}B^2L^{-1}RU^{-1}$.

10.5 Rotate $\boxed{URB}$ and $\boxed{URF}$ In Place

$\boxed{URB}$, $\boxed{URF}$ → $\boxed{RBU}$, $\boxed{RFU}$: $FD^2F^{-1}R^{-1}D^2RUR^{-1}D^2RFD^2F^{-1}U^{-1}$.