Introduction to Group Theory

By Rachael Schwartz

How many ways are there to arrange a collection of items? You've probably encountered this question before; it often appears in basic math problems for elementary school students. Innocuous as it seems, we will see that the problem of arrangements underlies one of the richest and most important areas in abstract mathematics. Its applications ripple through physics, molecular chemistry, image processing technology, quantum mechanics, and cryptography.

Let's begin by posing our question in a more precise way. For any positive integer n, we want to determine all possible ways for n distinct items to be placed into an ordered set.[1] Placements of these items must adhere to two rules: First, a single spot in our set may not contain more than one item; Second, every spot must be filled. To illustrate, consider the case where $n = 3$. We have an empty, "unarranged" set of three items, $\{\_\_, \_\_, \_\_\}$, and we want to determine all possible ways to place the items $1, 2, 3$ into this set.

There are multiple ways to solve this problem, and we need to select our method carefully. One could easily write out all possible arrangements of $1, 2, 3$ and find that there are six: $\{1, 2, 3\}$, $\{1, 3, 2\}$, $\{2, 1, 3\}$, $\{3, 1, 2\}$, $\{2, 3, 1\}$, and $\{3, 2, 1\}$. This answer is correct, but such a straightforward approach does not provide us with enough information to make the problem interesting. Not only do we want to calculate all possible arrangements of $1, 2, 3$, we want to define useful mathematical relationships between these arrangements.[2]

The crucial observation needed to define such relationships is that any arrangement can be converted into any other arrangement by relocating certain items within the arrangement. For instance, $\{2, 1, 3\}$ can be converted into $\{3, 1, 2\}$ by sending 2 to 3's location and vice versa, and $\{3, 1, 2\}$ can be converted into $\{2, 3, 1\}$ by sending 1 to 2's location, 2 to 3's location, and 3 to 1's location.

The conversion of one arrangement into another can be easily formalized using functions.[3] An arrangement function will take an arrangement as input and relocate items within the arrangement, thereby outputting another arrangement. To convert $\{2, 1, 3\}$ into $\{3, 1, 2\}$, we define a function f as follows:

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

To convert $\{3, 1, 2\}$ into $\{2, 3, 1\}$, we define a function g such that:

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

[1] An ordered set is simply a set whose elements are ordered. Specifically, a set S is ordered if for all elements a and b in S, exactly one of the following is true: $a < b$, $b < a$, or $a = b$. In our sets of arrangements, we order items from least to greatest, left to right.

[2] In mathematics, a set whose elements can be formally related to one another is said to have *structure*. The structure of a set applies to all elements in the set, is usually defined by some operation on the set, and will adhere to certain properties. Structures are typically defined by their properties.

[3] See endnotes for the formal definition of a function.

It turns out that there are six distinct functions that describe all possible conversions of one arrangement of $1, 2, 3$ into another:[4]

()	leaves the arrangement unchanged
(12)	swaps locations of 1 and 2
(13)	swaps locations of 1 and 3
(23)	swaps locations of 2 and 3
(123)	sends 1 to 2's location, 2 to 3's location, and 3 to 1's location
(132)	sends 1 to 3's location, 3 to 2's location, and 2 to 1's location

Applying these functions to any arrangement of $1, 2, 3$ will give another arrangement of $1, 2, 3$, and applying two different functions to the same arrangement will always produce two different arrangements. This means that applying each of these functions to any particular arrangement of $1, 2, 3$ will give us all six arrangements of $1, 2, 3$. This is not unique to the case of $n = 3$; we can find such functions for every positive integer n. Importantly, the function () is included in the set of arrangement functions on n items for every n.

Arrangement conversion functions share three important qualities. First, no two items are sent to the same location in the arrangement; Second, every location in the arrangement is occupied by an item after a function is applied; Third, every function intakes a set of three items and outputs the same set of three items.[5] Notice that the first two qualities are equivalent to the rules we used to define placements of n items into an ordered set. When a function has these two qualities, we call the function a *bijection*.

By this definition, bijections can only be established between two sets that contain exactly the same number of items. This is because bijective functions pair each item in the input set with exactly one item in the output set and leave no items in either set unpaired.[6] Since arrangement conversion functions input and output the same set of items, we call them *bijections from a set* (of n items) *to itself*. The formal name for an arrangement conversion function is a *permutation* on a set of n items.

※ ※ ※ ※ ※ ※

We will return to permutations shortly, but we now turn our intention to one of the most important structures in mathematics: groups. Given a set G and a mathematical operation

[4]Note that function (23) is the same as function f described above, and function (123) is the same as function g.

[5]It is crucial to distinguish between sets of items and arrangements of items. Two different arrangements of items $1, 2, 3$ are two different orderings of the same set, not two different sets. An arrangement conversion function changes the ordering of items in a set; it does not create a new set of items.

[6]Bijections are powerful tools in mathematics because they enable mathematicians to determine how many elements are in a set. If A and B are sets and the number of elements in A is known, then finding a bijection from A to B proves that B has the same number of elements as A. This proof technique garners amazing results; for instance, it shows that there are as many real numbers between 0 and 1 as there are real numbers between $-\infty$ and ∞.

denoted $\odot$,[7] we say that G *is a group under operation* $\odot$ if the following four rules are satisfied:

1) If a and b are any elements in set G and $a \odot b = c$, then c is always an element in G.
2) If a, b, and c are any elements in G, then the equality $a \odot (b \odot c) = (a \odot b) \odot c$ is always true.[8]
3) G contains one (and only one) element e, such that for any a in G, $a \odot e = a = e \odot a$. e is called the *identity element* of G.
4) For every element a in G, there is one (and only one) element z in G such that $a \odot z = e = z \odot a$. We say that a and z are each other's *inverses* in G.

These four rules are called *closure*, *associativity*, *identity*, and *inverse*, respectively.

These definitions can be hard to understand without context, so let's look at a simple example. We will use our four rules to prove that the set of all integers $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$ (commonly denoted as $\mathbb{Z}$) is a group under the operation of addition (denoted $+$).

First, we know that the sum of any two integers is also an integer, so $\mathbb{Z}$ is closed under $+$. Second, associativity is an algebraic property of integer addition, so $\mathbb{Z}$ is associative under $+$. Third, for any integer a, 0 is the only integer such that $a+0 = a = 0+a$, so 0 is the identity element of $\mathbb{Z}$ under $+$. Fourth, for any integer a, we have that $a + (-a) = 0 = (-a) + a$, so every integer has an inverse under $+$. Therefore $\mathbb{Z}$ is a group under addition.[9]

Due to the simplicity of the definition, there are *many* pairs of sets and operations that can be classified as groups. Yet when mathematicians study similarities and differences between various groups, the sets and operations themselves become relatively unimportant. Mathematicians focus mainly on the *structure* of a group; that is, the way that elements in set G are related to one another by operation $\odot$. Two groups may have no structural similarities, have some structural similarities, or have identical structures. When two groups have identical structures, we say that they are *isomorphic*.

Formally, an isomorphism between a group G with operation $\odot$ and a group H with operation $\otimes$ is an *operation-preserving bijection* f from G to H. When we say that f is an operation-preserving bijection, we mean that f is a bijective function, and that if a and b are in set G, then $f(a \odot b) = f(a) \otimes f(b)$. That is, if two elements in G are in some way related under operation $\odot$, then f sends these elements to two elements in H that are related in the same way under operation $\otimes$.

Again, this definition is best explained through example. We will show that the group of all integers $\mathbb{Z}$ under addition is isomorphic to the group of all even integers $2\mathbb{Z}$ under

[7] Addition, subtraction, multiplication, division, and exponentiation are examples of basic mathematical operations. We use the $\odot$ notation to discuss any operation, without specifying one in particular.

[8] On both sides of this equation, elements a, b, and c appear in the same order. In groups, we do not assume that $a \odot b$ is equivalent to $b \odot a$.

[9] However, $\mathbb{Z}$ is *not* a group under the operation of multiplication, because 1 is the identity element under multiplication, and for an integer a, the expression $a \times b = 1$ is only true when $b = \frac{1}{a}$. Therefore b not an integer unless $a = 1$, so the group of integers does not contain integer inverses under $\times$. This means that the group inverse rule is not satisfied, and $\mathbb{Z}$ is not a group under $\times$.

addition.[10] First, we establish a bijection f between $\mathbb{Z}$ and $2\mathbb{Z}$. Define a function f such that for any z in $\mathbb{Z}$, $f(z) = 2z$. No two different integers are sent to the same even integer, and every even integer is mapped to by some integer, so f is a bijection. Next, we prove that f is operation preserving. Let x and y be any integers. By the distributive law for integer addition, $2(x + y) = 2x + 2y$, so f is operation-preserving. We have thereby established an isomorphism between $\mathbb{Z}$ and $2\mathbb{Z}$.[11]

As you may have already guessed, the set of permutations (arrangement functions) for a collection of n items is a group under the operation of function composition.[12] Let P_n be the set of all permutations on a collection of n items (e.g., $P_3 = \{(), (12), (13), (23), (123), (132)\}$). Recall that applying any permutation in P_n to an arrangement of n items gives another arrangement of n items. This suffices to show group closure of P_n under function composition, since the composition of two permutations in P_n is another permutation in P_n. Function composition is always an associative operation, so P_n satisfies group associativity. We've noted that the permutation () is in P_n for every n; composing () with any permutation p in P_n leaves p unchanged, so () is the identity element in P_n. Because P_n is the set of *all* permutations on n items, for every permutation in P_n, there is another permutation in P_n which acts to reverse the first permutation. Therefore P_n satisfies the group inverse property (in P_3, permutations (), (12), (13), and (23) are their own inverses, and (123) and (132) are each others' inverses). Hence, P_n is a group.

※ ※ ※ ※ ※ ※

One of the most useful and versatile topics in group theory is that of symmetry groups. A *symmetry* of an object O is any transformation of O that preserves certain properties of O. For any object O, a *symmetry group* of O is any set of symmetries of O that form a group under the operation of composition.[13] Here, the word "object" is used very loosely, since the concept of symmetry has diverse and far-reaching applications.

In physical space (i.e., 2D, 3D, etc.), we define symmetry to be spatial transformations that preserve distances in space with respect to a given object. For example, rotating a circle around its center preserves the distance between any two points on the circle, so rotation is a symmetry of a circle in 2D space. All possible rotations of a circle (that is, all possible angles of rotation, from 0° to 360°) is a group under composition. A more complex example is the Rubick's Cube, whose symmetries are all possible moves that can be performed such that the Rubick's cube is still a cube. The Rubick's cube can be solved by studying its symmetry group under composition of moves. The study of spacial symmetry groups is integral to

[10] The proof that $2\mathbb{Z}$ is a group under $+$ is almost identical to the proof we discussed for $\mathbb{Z}$ under $+$.

[11] A fascinating consequence of this isomorphism is that there are as many integers as there are even integers. See footnote 6.

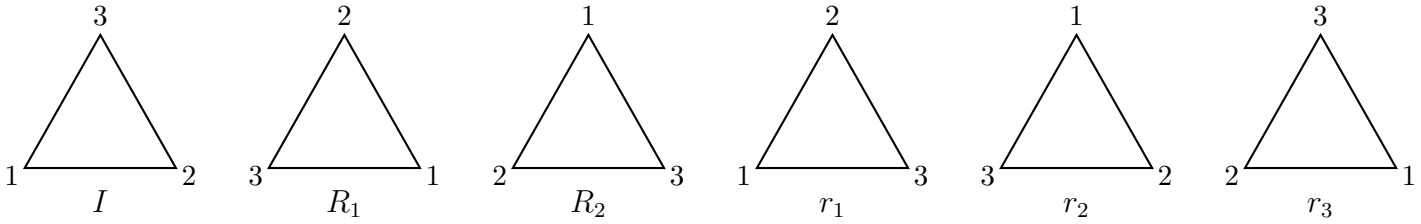
[12] Function composition is the application of one function f to the result of another function g. That is, if G is a set and x is an element in g, then the composition of f and g is $f(g(x))$. When f and g are combined in this way, the result is a new function h, such that $h(x) = f(g(x))$. We do not assume that $f(g(x)) = g(f(x))$; that is, applying f to the result of g is not necessarily the same as applying g to the result of f.

[13] Composing symmetries of O means applying the symmetries to O one after another.

chemistry and materials science, because molecules and crystal structures are described and classified by their symmetry groups in 3D space.

The concept of symmetry is further abstracted in physics, where it refers to the preservation of physical properties such as energy, time, momentum, and electromagnetism in a physical system. An incredible insight in physics came from mathematician Emmy Noether, who proved that any symmetry corresponds to a physical conservation law. For example, the symmetry group of spatial translations (i.e., moving from one point in space to another) conserves momentum, so the translational symmetry corresponds to Newton's first law of motion. Symmetry groups are also fundamental to quantum mechanics in ways far too advanced for our discussion.

We are going to examine one of the simplest physical symmetry groups: the symmetries of an equilateral triangle. In 3D space, there are two types of transformations that preserve distance with respect to an equilateral triangle T: rotations and reflections.[14] Label the verticies of T as 1, 2, and 3, labelling counterclockwise. T has two symmetric rotations counterclockwise around its center: 120° and 240°, denoted as R_1 and R_2, respectively. (A rotation of 360° is the same as a rotation of 0°, so it can be ignored.) T has three symmetric reflections: over the line through vertex 1 and its center, over the line through vertex 2 and its center, and over the line through vertex 3 and its center, denoted as r_1, r_2, and r_3, respectively. We also consider leaving T unchanged to be a symmetry of T, and this is denoted as I. I is the identity element of T's symmetry group. To illustrate:



Notice that each of these symmetries can be interpreted as a change in the ordering of T's verticies. If we read the the vertex labels counterclockwise for each symmetry, we see that $I = \{1, 2, 3\}$, $R_1 = \{3, 1, 2\}$, $R_2 = \{2, 3, 1\}$, $r_1 = \{1, 3, 2\}$, $r_2 = \{3, 2, 1\}$, and $r_3 = \{2, 1, 3\}$. Then, the set of all symmetries of an equilateral triangle is the same as the set of all possible arrangements of three items! Moreover, if we start with the arrangement $\{1, 2, 3\}$, then we are able to define T's symmetries as the permutations in P_3, such that $I = ()$, $R_1 = (123)$, $R_2 = (132)$, $r_1 = (23)$, $r_2 = (13)$, and $r_3 = (12)$. It turns out that the group of T's symmetries under composition and the group P_3 under function composition are isomorphic groups.[15]

Amazing as this result is, it's only the tip of the iceberg. When studying groups of permutations, we often pay close attention to collections of permutations within the group that form a group themselves. Such a collection is called *subgroups*, because it is contained within a larger group while also satisfying all properties of a group itself (under the same

[14] By preserving distance, we mean maintaining the locations of T's verticies in space.

[15] For a complete proof, see the endnotes.

operation as the group in which it is contained). Any symmetry group is isomorphic to a subgroup of a group of permutations P_n in which some property of the n items is preserved by all permutations within that subgroup.

But that's not all. One of the most fundamental and incredible results in group theory is called Cayley's Theorem. Cayley's Theorem says that absolutely *every* group in existence is isomorphic to a subgroup of a group of permutations P_n. The problem of rearrangements therefore underlies every application of group theory we have seen.