Math From Scratch Lesson 6:
Your Locker Does *Not* Have A Combination

W. Blaine Dowler

November 29, 2010

Contents

1 Defining Permutations and Combinations

We have already defined sets of objects. The sets we have seen so far can be used to form *combinations* in the mathematical sense. In mathematics, a combination is a set of objects which may be collected in any order. In other words, $\{1, 2\}$ is mathematically identical to $\{2, 1\}$ as a combination. Mathematics also involves *permutations*, which are combinations where the order of the elements in a set does matter. It is for this reason that combination locks are misnamed: the order of the numbers is very important, so they are more properly called permutation locks.

As you may recall, in our definition of sets, we noted that order is irrelevant. How do we formally impose an order on the set? We use subsets. We can formally distinguish the permutations by replacing the second object in the set with an appropriate subset, as follows: $\{1, \{1, 2\}\}$. This imposes the distinguishing feature required for an imposed order: the element 1 is isolated, so that is our first entity. The second entity is defined by a subset with two objects; the "new" object is the one that comes second in our permutation. If we had a permutation of three symbols, we would require another subset. For example, the permutation of 1, 2 and 3 in order would be formally represented as $\{1, \{1, 2\}, \{1, 2, 3\}\}$. The third object is the one in the set of three objects.

Permutations can be naturally represented using group theory.

2 Counting Permutations

Imagine there are five people racing to get in line for some sort of ticket sales. If there are only five seats left, then there are several different arrangements of individuals. They could arrive in alphabetical order (Bruce, Donald, Henry, Janet and Tony), age order (Tony, Donald, Henry, Bruce and Janet), height order, and so forth. In fact, there are 120 possible ways for these five people to line up!

We count these possibilities by counting choices. There are five possibilities for the first person to arrive. Once that person is in line, there are only four possible people who can come next, three choices for the person in the middle of the line, two for the fourth person in the line, and only one choice left for whoever comes last in line. To count, we multiply these numbers together: $5 \times 4 \times 3 \times 2 \times 1 = 120$.

2.1 Factorials

Factorials are a compact means to express such counting. Permutations frequently involve the product of every natural number from a starting point n down to 1. We write this compactly as a factorial, using an exclamation point:

$$n! = n \times (n-1) \times (n-2) \ldots 3 \times 2 \times 1$$

This notation will recur several times in the future.

3 Expressing Permutations

Imagine we have a particular lineup of our five people. We wish to have a different lineup. We could express any desired lineup (permutation) as a transformation of the original lineup. Let us take the two examples above, and transform the alphabetical ordering into the age ordering. We start with the lineup "Bruce, Donald, Henry, Janet and Tony" and look at what we have. We can move people around in pairs. We can start by putting Tony at the front of the line, which we accomplish by swapping Bruce and Tony. Donald is right where we want him, so we leave him alone, as is Henry. For the final step, Bruce and Janet trade places.

The typical notation for permutations deals with these transformations. Let the alphabetical order be represented as 12345. We can represent transformations by putting combinations of these numbers in brackets: our original transformation of trading Bruce and Tony would then be written as (15). Our second transformation, trading Bruce and Janet, would be written (41). Note that Bruce is still denoted by 1. The fact that he moved doesn't change his assignment in this fashion.

We can write these two transformations together. Remembering that, in algebra, the rightmost object acts first, the total transformation is written (41) (15). There is also a way to represent the complete transformation as a single object: given that we transformed 12345 into 52314 in our transformation, we ultimately replaced 1 with 5, 4 with 1, and 5 with 4. As a single entity, this is written (154). (If you read this as "one replaces five, which replaces four, which replaces one" then we seem to have an inconsistency in notation, as the cycle would be read from left to right. Instead of the verb "replaces," think with the phrase "is replaced by" and it will realign as anticipated: "four is replaced by five, which is replaced by one, which is replaced by four.") This can also be written as (541) or (415). All three are interchangeable; the first element is replaced by the second element, the second by the third, and so forth, until the last element in brackets is replaced by the first.

4 Exponents

In the interest of efficient notation, the concepts of exponents will be introduced here. An exponent is merely shorthand for repeated multiplication. For example, $x \cdot x \cdot x = x^3$. The exponent, written as a superscript immediately to the right of a variable or other mathematical object, indicates the number of copies of that object being multiplied together.

5 Permutations as Groups

Now that we have a formal mathematical language to describe permutations, we can approach the question of whether or not permutations constitute groups.

1. **Defining The Algebra** We start by identifying our potential algebra. Let P_n be the group of permutations[1] on n symbols. Let the operation on the group be neither addition nor multiplication, but rather the sequential application of permutations. Let us now test whether or not this behaves as a group.

2. **Identity** The identity axiom is typically checked first because it is often the easiest axiom to check. If it fails this test, no further evaluations are necessary. In this case, the identity element e on the group of permutations of n symbols is the permutation in which no transformations occur. Although it is typically written as e or as some other simple symbol, one can think of it as $(11)(22)(33)\ldots(nn)$ just as easily. It's a lengthy and redundant notation, but it drills home the fact that e is, in itself, a permutation.

3. **Inverses** The test for the existence of inverses is surprisingly easy, and quite revealing. If x is a permutation with a single pair of brackets enclosing i symbols, then the inverse of x is x^{i-1}. This relationship is easiest to see with a concrete example. Let us take the permutation (12345) on P_5. If we multiply it by itself, we get $(12345)\,(12345) = (13524)$. In other words, the first copy of (12345) transforms 1 into 2, and the second copy transforms 2 into 3, thus transforming 1 into 3 overall. A third application results in (14253), and a fourth application results in $(15432) = (54321)$. A fifth application cancels completely, thus becoming e. If you cycle n symbols n times, there is no change overall. Thus, cycles with two elements, such as (12), are their own inverses.

4. **Closure** The algebraic objects were are defining are all transformations on the same n symbols. Regardless of how these symbols are arranged or rearranged, any combination of them will still be a transformation on those n symbols. This algebra is closed. (For example, no amount of rearranging objects 1, 2 and 3 will transform object 5 in any way, as all of our transformations are based on symbols trading places with each other. There is no "move to the front of the line" object.)

5. **Associativity** Remember, associativity does not refer to the order transformations are applied, but to the fact that simplifying compound transformations into a single (or, at least, smaller number) of transformations

[1] As confusing as it is, it is customary to use the word "permutation" to represent both the order of objects and the transformation between orders. From now on, we will use the word to refer to the transformations.

does not depend upon the order in which they are simplified. For example, take (12)(13)(14)(24) as our collection of transformations. Simplifying this collection from right to left gives us:

$$\begin{aligned}(12)(13)(14)(24) &= (12)(13)(214)\\ &= (12)(1423)\\ &= (14)(23)\end{aligned}$$

Notice that this simplified to a pair of transformations. Each pair is a closed cycle; this complete transformation causes two pairs of numbers to trade places. Now, simplifying from left to right, but still applying the rightmost transformation first, we find:

$$\begin{aligned}(12)(13)(14)(24) &= (132)(14)(24)\\ &= (1432)(24)\\ &= (14)(23)\end{aligned}$$

The intermediate steps appear different, but the final result is the same. One could simplify the middle pair first, with the intermediate step (12)(143)(24), or even simplify the leftmost and rightmost pairs simultaneously for an intermediate (132)(142) and still arrive at the same final result.

Although the proof lacks rigor, particularly with the associative property, it at least seems very likely that the group of permutations on n symbols forms a group. A fully formal treatment bears this out; the typical notation is S_n, referring to this as the symmetry group.

6 Generators

In the previous lesson, we reduced the group of symmetries in an isosceles triangle from six unique symbols to combinations of the three symbols e, x and y. These three symbols can be combined to *generate* the entire group. Now, we don't particularly want to invent 120 different symbols for the elements of S_5, or (worse yet) 3628800 symbols for S_{10}. This begs the question: can some smaller set of elements be used to generate the larger set?

The answer is that, yes, this can be done. Logic dictates a simple method: define the symbols $e, (12), (13), \ldots, (1n), (23), (24), \ldots, (2n) \ldots$ first. With every pair of transformations defined, as well as the identity element, we can create

any transformation as a combination of these elements. In most symmetry algebras, however, there are even smaller sets which can generate the complete list.

The above logic would reduce S_3 to four generating elements: $e, (12), (13), (23)$. We can simplify this down to two elements. The first element we can drop is e. This is surprising at first, given the importance of e to defining S_3 as a group, but it does work. Remember, by taking e out of the list, we are not saying that we are taking e out of the group, but that we can make the e element out of the elements still on our list. In fact, the rest of our list is made of cycles that cycle through two numbers each, called pairwise transformations. Any pairwise transformation, when applied twice, becomes the identity element. ($(12)(12) = e$, for example). We are now down to three generators, but will soon remove one from the list. The element (23) can be made from the other two as follows:

$$(12)(13)(12) = (12)(123) = (23)$$

As the element (12) cannot, in any way, be used to produce (13) on its own, the two generator list $(12), (13)$ is as small as our generator list can get. Of course, this is not the only way to express the generators of the group. We could also use $(12), (23)$ or $(13), (23)$ for generators in the same manner. Beyond that, would could use $(123), (12)$ to generate the group, if we are able to prove that (13) and (23) can be expressed as a combination of these. Observe:

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

This produces our first element. Now, we could now produce (23) as before through a combination of (12) and (13), and strictly speaking that's all we have to do, but we could also compute this:

$$(12)(123) = (23)$$

Thus, we see that our list of generators is not unique, but contains fewer elements than the entire group. (For S_3, we took a group of size $3! = 6$ and boiled it down to 2 generators.)

So, how many generators do we need for, say, S_4? Instinct says 3: $(12), (13), (14)$

by the above logic. Let's see what we can do starting only with (1234) and (12).

$$\begin{aligned} e &= e \\ (12) &= (12) \\ (12)(1234)(1234)(12)(1234) &= (13) \\ (12)(1234)(12)(1234)(1234) &= (14) \\ (1234)(1234)(12)(1234)(12) &= (23) \\ (1234)(12)(1234)(1234)(12) &= (24) \\ (23)(24)(23) &= (34) \end{aligned}$$

The two elements (1234) and (12) alone are sufficient to generate all pairs of transformations. With sufficient patience, one can find combinations of these two generators which lead to all other elements of S_4.

7 S_n and Regular Polygons

In the previous lesson, we defined the group which describes the symmetries of an equilateral triangle, and it had six elements and two generators. In mathematical terms, this is called an *isomorphism*[2], because the two entities have the same basic form. If we label the triangle's three corners as 1, 2 and 3, then each reflection along a line of symmetry can be represented by a permutation of a pair of elements, while each rotation can be represented as a permutation of three elements. This begs the question: if S_3 is an isomorphism of the symmetries of a triangle, might S_4 be an isomorphism of the symmetries of a square, and so on?

Let us begin the exploration with square as in figure 1.

A simple clockwise rotation can be represented by (1234). There are also four lines of symmetry: reflections about the diagonal lines of symmetry can be represented by (13) and (24). Reflection about the vertical line of symmetry is represented by (12)(34), while reflection about the horizontal line of symmetry is represented by (14)(23). Can these elements (or combinations of them) be used to generate every possible permutation on the symbols 1, 2, 3 and 4? The answer may surprise you: although these geometric transformations can be used to generate a complete group algebra, that group is *not* isomorphic to S_4. The geometry of a square is restricted to those transformations which result in a square after transformation, while the permutation group S_4 does not

[2] *iso-* meaning same, *-morph-* meaning form, *-ism* which acts to indicate the noun which is the condition or state of being which satisfies the previous descriptors in the word. Thus, an isomorphism is an object with the same form as another object.

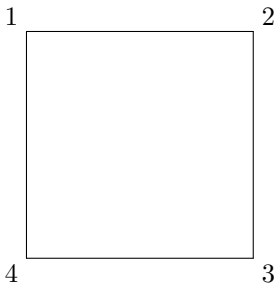

Figure 1: A square.

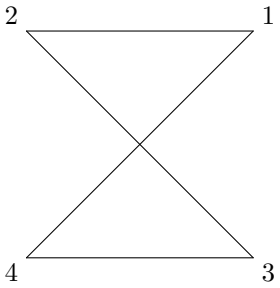

Figure 2: Not a square.

have that restriction. Visually, the problem comes from pairwise permutations on consecutive symbols, such as (12), which lead to pictures such as that in figure 2.

Such transformations change the geometric label assigned to the figure in question, and are not permitted by geometric symmetry operations. Of the $4! = 24$ possible permutations of four symbols, only 8 may be used to represent the symmetries of a square. Of the remaining 16 permutations, 8 create figures such as figure 2, and 8 produce figures such as figure 3.

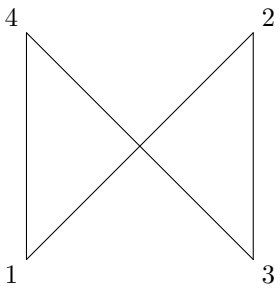

Figure 3: Also not a square.

The fundamental differences between these three figures can be seen in the order of the elements: in the original square, 1 appears between 2 and 4. In figure 2, 1 and 2 are still adjacent labels, but 1 and 4 are no longer adjacent. Similarly, in figure 3 1 and 4 are still adjacent, but 1 and 2 are not. As an intuitive but informal criteria, we can think of the transformations which correspond to the geometry of regular polygons to be those which preserve each label's neighboring labels.[3]

8 Upcoming Lessons

What we have seen above is one of our earliest examples of a subgroup: a group within a group. Our next lesson will be devoted to the properties and identification of subgroups.

[3]The group of symmetries of a triangle and S_3 are completely identical because it is not possible to create a "twisted" triangle in this fashion; the neighbors of any given label cannot be changed with only three labels.