Math From Scratch Lesson 007: In Her Majesty's Secret Subgroup

W. Blaine Dowler

November 24, 2010

Contents

1 Defining Subgroups

We have already seen that every element in the group defining the symmetries of a geometric square can also be represented by members of the much larger group S_4, defining the permutations of four symbols. This is far from the only such group that can be found inside another group. [1]

So what, then, is a subgroup?

[1] In fact, the group of symmetries on a square has several subgroups of its own: the group formed by the identity element alone, the group formed by any one of the four reflections along with the identity element, and the group formed by the identity element and all rotations.

Going back to the notation from lessons 2 and 4, defining sets and groups, we have the following:

Definition If the set G forms an algebraic group when combined with the operation $\cdot$, then we can form a subgroup $(H, \cdot)$ if the following conditions are met:

1. Every element in the set H is also in the set G. Formally: $\forall h \in H, h \in G$. Note that the converse is *not* required: it is not only permitted, but extremely common for G to have elements that are not elements of H. (In our example of a square, the "twisted" shapes fall into this category.)
2. The operation $\cdot$ is defined for elements of H.
3. $(H, \cdot)$ is, itself, a group, satisfying all four axioms.

2 Verifying Subgroups

Now that we know what we are looking for, how do we efficiently test to see if something is a subgroup of another group? Retesting all group axioms, verifying the operation, and checking that every element of H is an element of G sounds time consuming. Thankfully, we can skip a few steps, by showing that some properties of $(G, \cdot)$ will be inherited by $(H, \cdot)$.

The first requirement ($\forall h \in H, h \in G$) is one that is relatively easy to test in most cases. The definitions of H and G will often make this obvious. For example, if G is the group of all symmetries of a geometric square, and H is the set of all rotations and the identity transformation of a square, then it is relatively obvious that every element of H is an element of G. Unfortunately, there is no single approach to verifying this property; it must be handled on a case by case basis. For example, if one intends to show that the set of symmetries of a geometric square H forms a subgroup of $S_4 = G$, then one needs to systematically match each element of H to an element in G by drawing the original square, labeling the corners, performing all symmetry transformations, and then matching the new arrangement of corner labels to the corresponding permutation.[2] This step is sometimes tedious, but rarely is it particularly difficult.

The second requirement, that the operation $\cdot$ is defined for elements of H, is immediately inherited once the first requirement is established. It has already

[2] In this case, using the labels from the previous lesson, we see that a clockwise rotation by a quarter turn is the permutation (1234), the reflection about the vertical axis of symmetry is given by (12)(34), a rotation by half a turn is given by (13)(24), and so forth.

been established for $(G, \cdot)$, so if we've proven that $\forall h \in H, h \in G$, then this follows naturally, and needn't be explicitly checked.

The third requirement is actually four distinct axioms, some of which need to be checked:

1. **Identity**: Though the existence of the identity axiom is listed third in our definition of a group, it is typically the first to be checked in this process, as it is generally the easiest to prove or disprove.
2. **Associativity**: This is immediately inherited from $(G, \cdot)$, and does not need to be explicitly checked.
3. **Closure**: If $a \in H$ and $b \in H$, then is $a \cdot b \in H$? This needs to be checked explicitly. This is also why the above list of subgroups of the symmetries of a square listed "the group formed by *any one* of the four reflections along with the identity element" instead of simply any combination. If $(12)(34) = a$ is the reflection of the square about the vertical axis of symmetry, and $(14)(23) = b$ is the reflection about the horizontal axis of symmetry, then $ab = (12)(34)(14)(23) = (13)(24)$, which is not in the set $\{e, a, b\}$.
4. **Inverses**: In short, if $h \in H$, then is $h^{-1} \in H$? This one must also be explicitly checked.

Once these tests are established, we can determine whether or not something is a subgroup of another group.

3 Cyclic Groups and Subgroups

Many of the most interesting subgroups are *cyclic* groups, particularly when they contain a finite number of elements.

A cyclic group is one with only one generator, as defined in the previous lesson. If there are n elements in a group with only one generator x, then $x^n = e$, guaranteed, leaving $x^{-1} = x^{n-1}$. If we define our group as the rotations of a square, then x would be the clockwise rotation through a quarter turn. We then have the following, using the notation of the permutation group S_4:

1. $x = (1234)$
2. $x^2 = (1234)(1234) = (13)(24)$

3. $x^3 = (1234)(1234)(1234) = (1234)(13)(24) = (4321)$

4. $x^4 = (1234)(1234)(1234)(1234) = (1234)(4321) = e$

Thus, our group consists of the four elements $\{e, x, x^2, x^3\}$, where x is the inverse of x^3 and vice versa, and x^2 is its own inverse. This is called a cyclic group because you can cycle through every element in the group through repeated multiplication by a single element x. We could also form the cyclic group using x^3 as the generator; in the geometric interpretation, x^3 is the counterclockwise rotation through a quarter turn. As geometry has no preference for direction of rotation, this makes perfect sense. However, we may *not* use x^2 to generate the group; as it is self inverse, it would generate the two element group of $\{e, x^2\}$ instead. In other words, our subgroup has a subgroup. This subgroup also has a subgroup: the group $\{e\}$ is a perfectly valid (if trivial) subgroup of every conceivable group, and is the only valid group containing exactly one element.[3]

4 Order

The term *order* has two different definitions in group theory, depending upon whether that term is being applied to the group or to an element of the group.

4.1 Order of a Group

The *order of a group* is the number of elements within that group. Thus, the order of the group describing the symmetries of a geometric square is 8, while the order of S_4 is 24. There is no requirement that a group has finite order; in other words, there is no limit to the number of elements one can place inside a group. The order of a group is also referred to as the *cardinality* of a group.

4.2 Order of an Element

The *order of an element* x in a group is the smallest natural number n which satisfies $x^n = e$. (Remember, the set of natural numbers does not include 0.) The order of e, for example, is 1 in all groups, as $e^1 = e$. The definition specifies the smallest natural number to avoid ambiguities from situations such as $e^2 = e^3 = e^4 = \ldots = e$. In a group of finite order, every element will have

[3]The group $\{e\}$ is also the only group that can be studied in totality in seconds by even the newest student of group theory.

finite order. Note that there is *no* requirement that elements of an infinite group have finite order. It can happen, but it is certainly not required.

4.2.1 Proof by Contradiction

In the case in which our group G is a cyclic group, the order of the generator x ($o(x)$) will be the order of the entire group ($o(G)$). In all cases, $o(x) = o\left(x^{-1}\right)$. This may be proven using a technique called *proof by contradiction*: assume the opposite of what you want to prove is true, and show that it would lead to an inconsistent or broken system. In this case, we assume $o(x) = m \neq o\left(x^{-1}\right) = n$. Then it would be the case that $x^m \cdot \left(x^{-1}\right)^n = e \cdot e = e$. By the associative property, we could start canceling out x and x^{-1} terms in pairs from the middle of this construction, so that one iteration later, we would have $x^{m-1} \cdot \left(x^{-1}\right)^{n-1} = e$. After successive applications, we would be left with either $x^{m-n} = e$ or $\left(x^{-1}\right)^{n-m} = e$, depending upon the individual values of m and n. In either case, we would have a single element raised to an exponent that is less than its order, and this would be equal to the element. As the order of an element is the smallest possible exponent satisfying this condition, we have a contradiction. The only questionable part of this calculation was our assumption that $o(x) = m \neq o\left(x^{-1}\right) = n$. This assumption must be invalid, and the only piece of the assumption that isn't justifiable is the inequality of $m \neq n$. Thus, we cannot use this assumption, and we must have $m = n$, or $o(x) = o\left(x^{-1}\right)$. Note also that we can use this to imply that, for elements of an algebra which have inverses, we can now prove that $x^0 = e$ regardless of x.

5 Partitions

Let us return to the group S_3, which described the symmetries of an equilateral triangle.. That group had two generators, x and y, such that $o(x) = 3$ and $o(y) = 2$. The entire set can be written as $\left\{e, x, x^2, y, xy, x^2y\right\}$. Notice that the first three symbols can create a cyclic subgroup of their own as $\left\{e, x, x^2\right\}$. This leaves the set $\left\{y, xy, x^2y\right\}$ behind. This set does *not* form a group. It is still associative, and it still has inverses, but it is not closed because it lacks the identity. Thus, this is a set, but not a subgroup or any other kind of group.

So, then, what is the point of making note of this set? At times, we wish to look at elements of an algebraic set which have some sort of property in common, but which do not form an algebra themselves.[4] This is where partitions come into play.

[4]Common examples not yet formally defined in these lessons include the even numbers, multiples of any natural number higher than 1, and so forth.

Definition A *partition* of a set S is a collection of subsets T_i meeting the following criteria:

- The subsets are *disjoint*. In other words, each element of S appears in at most one subset T_i. Formally written, if $x \in T_i$ and $x \in T_j$, then $i = j$. Alternatively, using the intersection notation from lesson two and logical symbols from lesson one, we can write this requirement with the statement $\forall i, j : T_i = T_j \wedge T_i \cap T_j = \{\} = \emptyset$.
- Every element $x \in S$ appears in at least one subset T_i.
- No subset T_i is empty.

With these two combined properties, we see that every element $x \in S$ appears in exactly one subset T_i. Again, using formal set theoretical notation, we can establish this without the use of the element x by simply writing the two conditions $\forall i, j : T_i = T_j \wedge T_i \cap T_j = \emptyset$ and $S \cup_i T_i$. The first condition is as above; the second indicates that the union of all sets T_i (i.e. the set formed by everything that is a member of at least one T_i) is the set S.

There is an interesting implication here: when a set has been partitioned, there is a *maximum* of one subset T_i which can form the set within a subgroup. This is because a maximum of one subset will contain the identity element. Note that there is no requirement that there is any subset which can form a subgroup at all: we could well define on subset of S_3 as $\{e, x\}$. As this set lacks $x^2 = x^{-1}$, it cannot be a group or subgroup in its own right.

Note that there is no particular requirement that every T_i is the same size. We will soon discover (in another lesson) a situation in which that requirement does lead to some interesting implications. Finally, note that there is no requirement that either S or any given T_i has a finite order.

6 Equivalence Relations and Classes

In our first lesson, we defined equivalence relations, but have not referred to them since. To quickly recap, using the notation $\sim$ for an equivalence relation, we recall that an equivalence relation is defined by three properties:

1. **Reflexivity**: $x \sim x$
2. **Transitivity**: $a \sim b$ and $b \sim c$ combined imply $a \sim c$
3. **Symmetry**: $a \sim b$ implies $b \sim a$

Note the absence of our fourth property, antisymmetry: it is possible for two distinguishable elements to be equivalent, even though they cannot be equal. Note also that we have various terms to use to describe an equivalence relation: if $x \sim y$, then we can say "x is equivalent to y" or "x is similar to y."

So, how does this relation to partitions in any way? The simplest definition of an equivalence relation which is not equality is to define them by the subsets they belong to within a partition. So, in this example, if $x \sim y$, if $x \in T_i$ and $y \in T_j$, then we must have $i = j$. This is what we use to define an *equivalence class*: if we arbitrarily choose x to represent the set T_i that it belongs to, then the equivalence class $[x]$ is defined as follows: $[x] = \{y : x \sim y\}$. In other words, $[x]$ is the set containing every element which is similar to x, which means $[x]$ is just another way to write the T_i that x is a member of. This notation is a little more clear about which partition is which, particular when we are using a rigorous rule to build our partitioning sets. It will be the preferred notation in the future.

7 Upcoming Lessons

Next, we will define mappings and cosets[5], which will lead us directly into Lagrange's Theorem. After that, we will set group theory aside for a while to begin ring theory.

[5]It is when defining cosets that we will find partitions in which every T_i has the same order.