Groups for Non-"Math People"

Dennis Leet

April 2018

1 Introduction

It is with great excitement that I am presenting this important information on cosets and groups to you! I understand that many of you consider your mathematical prowess to be lacking - and honestly, I often feel the same way. My goal with this writing is to give you a hands on approach to cosets and some of their most important properties. I will be using examples and proofs. But fear not! I have worked my hardest to make these examples as accessible as possible! I hope that you enjoy reading my overview as much as I have enjoyed writing it.

2 Definitions

In mathematics we accept certain things to be true and then build off of these accepted truths. These truths that we choose to accept are called axioms. Analogously, I will be asking you to accept a few definitions on which we will build our discussion of cosets.

Firstly we must understand that **Sets** are merely collections of objects. They are also objects in and of themselves. For instance, we could have a set $X = \{a, b, c\}$. In this case our set is named X and it contains elements – or members a, b, c.

Groups are sets which meet the following four criteria:
1) The set is closed under an operation.
2) The set is associative.
3) There exists an identity element in the set.
4) There exists an inverse for every element in the set.

While I do not mean to brush over the mechanics, for now I will simply ask you to accept these statements as the definition of a group. Essentially that a group is a special type of set with certain interesting characteristics. Now we have come to the definition which is most pertinent to our discussion. **Cosets** are defined as such. Consider any group G and subgroup of G which we will call H. We define the left coset of H, gH as any member of G operating on all members of H on the left. The right coset is defined in an opposite fashion and denoted Hg. Also, note that subgroups are subsets of groups that are themselves groups

Note that both gH and Hg are sets and notice that we place great emphasis on where the element of G is placed. It could be the case that gH and Hg are completely different sets! By different I mean that the objects contained in gH are not the same as the objects contained in Hg. The two sets could have no objects in common or could only be off by one element or more; either way they are not necessarily the same set. However, there are certain cases where the equation $gH{=}Hg$ is always true.

We call a group **normal** if $gH = Hg$ for every $g \in G$. Thus, if the left and right cosets contain the same elements, then we say that H is normal in G. An important idea comes into play which caused me great confusion when learning this subject. We <u>are not</u> saying that $gh = hg$ for a specific g and h.

Rather, we are just saying that when you take any member of G and operate it individually on each element in the set of H, you wind up with the same set - whether or not you go in from the right or from the left side. If H is normal in G, we denote it as $H \trianglelefteq G$.

Now take a step back for a moment. We know that a set is just a collection of objects and that a set is an object in and of itself. Since we are speaking of cosets, one has to ask if we could put all of these cosets together into a collection. The answer is yes. We call such collections with $H \trianglelefteq G$ **quotient groups**. Consider $\mathbb{Z}/3\mathbb{Z} = \{3\mathbb{Z}, 1+3\mathbb{Z}, 2+3\mathbb{Z}\}$. What this means is that we are partitioning the integers (positive and negative whole numbers including zero) into three distinct groups based on their remainder when divided by 3. For instance the number 7 is a member of $1 + 3\mathbb{Z}$, since 3 divides 7 with a remainder of 1. 30 resides in $3\mathbb{Z}$ since it is evenly divided by 3. Also, note that any given number n $\in \mathbb{Z}$ will exclusively reside in only one of the three cosets. We then say that the cosets form a partition of the group $\mathbb{Z}$ and that the quotient group is a group by itself. Think of it this way: we have taken the group of integers, partitioned them, and then when we collected the partitions found that they formed a group - wow!

Continuing the conversation and bringing together some of what we have just learned, lets take a look at the group of integers under addition. Looking back at our four main axioms for a group, we can see that $(\mathbb{Z}, +)$ satisfies these axioms. If you would like to double check you could. For instance, try to find two integers which add together to generate a non-integer entry (I bet you can't). Similar to $\mathbb{Z}/3\mathbb{Z}$, lets take a look at $\mathbb{Z}/10\mathbb{Z}$ specifically the $10\mathbb{Z}$ portion. This is a subset of the integers since is is all of the integers $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$ multiplied by 10. Thus $10\mathbb{Z} = \{..., -20, -10, 0, 10, 20, ...\}$. For reasons which will be clarified momentarily, lets show that $10\mathbb{Z} \leq \mathbb{Z}$ (that is math-speak for, "$10\mathbb{Z}$ is a subgroup of $\mathbb{Z}$". To prove that a subset is a subgroup we must show two important characteristics:
1) That the subset is closed under the given operation.
2) That every element in the subset has an inverse. Notice that we are only proving 1 and 4 of our four axioms to be a group. With that being said - lets get to the proof!

1)Closure: Let's consider two elements $a, b \in \mathbb{Z}$ where $a = 10n$, for some $n \in \mathbb{Z}$ and $b = 10m$, for some $m \in \mathbb{Z}$. We see that $a + b = 10n + 10m = 10(n + m) = 10(l)$, where $l \in \mathbb{Z}$ due to the integers being closed under addition. Thus two objects added together from $10\mathbb{Z}$ generate another object in $10\mathbb{Z}$.
2)Existence of inverses: Consider any $a \in 10\mathbb{Z}$. Since $a = 10n, n \in \mathbb{Z}$, what would happen if we added $-a$? Let's find out; $a + (-a) = 10n + (-10n) = 10n - 10n = 10(n - n) = 10(0) = 0$. Thus the inverse of any $a \in 10\mathbb{Z}$ is $-a \in 10\mathbb{Z}$. Our proof is complete as we have shown that $10\mathbb{Z}$ satisfies both axioms.

Lastly for fun, I will make the claim that $10\mathbb{Z} \trianglelefteq \mathbb{Z}$. Consider our definition of normal is that if the right and left hand cosets are equal or $gH = Hg$. By manipulating the equation with g^{-1}, we can make an equivalent statement that a set $H \trianglelefteq G$ if $gHg^{-1} = H$. Consider $a, a^{-1} \in \mathbb{Z}$ (noting that the inverse of any integer a under addition is $-a$) and lets look at $a + 10\mathbb{Z} + a^{-1}$:

$$\begin{aligned} & a + 10\mathbb{Z} + a^{-1} \\ &= a + 10\mathbb{Z} - a \\ &= a + (-a) + 10\mathbb{Z} \\ &= a - a + 10\mathbb{Z} \\ &= 10\mathbb{Z}. \end{aligned}$$

Therefore, $10\mathbb{Z} \trianglelefteq \mathbb{Z}$. As you can see the algebra around groups can either be very hands on or abstract. I hope to provide examples of both varieties as we continue.

3 It's Hip to be... Normal?

Yes indeed! Since we have defined groups as special sets and normal groups as being a special sort of group, it should then come as no surprise that there are some strings attached to $\mathbb{Z}/3\mathbb{Z}$ or any G/H being a group. This proof will seem abstract and I will attempt to break it down. We will begin by considering a group G and N; a subgroup of G (often denoted as $N \leq G$). We are interested in showing that the only way for G/N to be a group is if $N \trianglelefteq G$. Think back to those four requirements at the beginning of this paper concerning

a set being a group. If any of those are violated then G/H can not be considered a group. Also note what is meant by the first axiom that we accepted. Closure under an operation means that I can take any two element in the set, perform the sets operation on them and I will wind up with another element still in that set. Observe: Consider a group G with operation $*$ denoted as multiplication. Closure means that if we take a,$b \in G$ and then apply $*$ we will generate the following: $a*b=c$ where $c \in G$. c must be a member of G, otherwise the set is not closed under the operation. With this knowledge in tow, lets take a look at G/N.

Consider G/N. Specifically think of two elements in the set which we will call x and y. Also, tack on that G/N has some operation. This operation is defined as for any $x=aN$ $y=bN$, that $xy=aNbN=abN$. This operation only works if $N \trianglelefteq G$. Due to G being closed $ab=c$, $c \in G$. Thus the operation is closed as a member $c \in G$ is operating on the set N from the left.
Next consider any $aN, bN, cN \in G/N$. We see that;

$$\begin{aligned}&(aNbN)cN\\ =&abNcN\\ =&abcN\\ =&aNbcN\\ =&aN(bNcN).\end{aligned}$$

Thus we see that G/N is associative. For our inverse consider the element $eN \in G/N$. We operate this element with an arbitrary $aN \in G/N$. Observe:

$$\begin{aligned}&aNeN\\ &= aeN\\ &= aN.\end{aligned}$$

Lastly we want to see if an inverse exists for every element in G/N. Consider any arbitrary a and $a^{-1} \in G$ and the cosets $aN, a^{-1} \in G/N$. Consequently:

$$\begin{aligned}&aNa^{-1}N\\ &= aa^{-1}N\\ &= eN\\ &= N.\end{aligned}$$

Through proving our four important axioms, we have shown that G/N is a group.

4 Homomorphisms and Kernels

If you feel that we are getting into the nitty gritty of our work, then you are correct. I want us to explore the definitions of a homomorphism and the kernel. A **homomorphism** is a function or map from one group to another which accomplishes a few important tasks. Consider any two groups G and G'. A homomorphism from G to G' with respective operations $\square$ and $\triangle$, which we will denote as ϕ, is defined in the following manner: For any $a, b \in G$,

$$\phi(a\square b) = \phi(a)\triangle\phi(b).$$

Importantly, the homomorphism preserves the algebraic structure of the group. So, why do we care? Because these groups, due to their axioms, have structures bound to the four important criteria which make them groups. These criteria were outlined at the beginning of this paper. Please take a moment to review the following criteria for a group:

1) The set is closed under an operation.
2) The set is associative.
3) There exists an identity element in the set.
4) There exists an inverse for every element in the set.

These criteria rule all of the elements and bind them into acting a certain way. A group homomorphism seeks to preserve these axioms and keep the algebraic structure intact to boot.

Switching gears, the **kernal**, often identified as e, of any funtion ϕ is defined as:

$$\ker(\phi) = \{g \in G | \phi(g) = e'\}$$

Meaning that if we have two groups G and H and a function $G \xrightarrow{\phi} H$; the kernel is a collection of all of the elements which are mapped to the identity element in H. Specifically for group homomorphisms, the kernel of any ϕ: $G \xrightarrow{\phi} H$ is a subgroup of the group G. In fact, the kernal of a function is normal to the image of the function. To be more exact $ker(\phi) \trianglelefteq G$.

Let's once again take a step back and consider what we are trying to accomplish here. Our discussion is about groups, subgroups, and cosets. We would like to know if we already have a group G, are there ways to create more subgroups or are there hidden subgroups within G given certain criteria. Thus far we have used cosets to create subgroups with G/N given that $N \trianglelefteq G$. Also, our discussion of the Kernel has defined another normal subgroup which we could use to create a group of the form $G/ker(\phi)$, if ϕ is a homomorphism.

With that being said, we need to show that $ker(\phi) \trianglelefteq G$ for a group G. If this cannot be shown then $G/ker(\phi)$ is not a group. One of the ways that we can do this is to show that $gng^{-1} \in ker(\phi)$. Allow ϕ to be a homomorphism such that $G \xrightarrow{\phi} G'$ and consider the element gng^{-1}. Observe the following:

$$\begin{aligned}
&\phi(gng^{-1}) \\
&= \phi(g)\phi(n)\phi(g^{-1} \\
&= \phi(g)e_{G'}\phi(g^{-1}) \\
&= \phi(g)\phi(g)^{-1} \\
&= e_{G'}.
\end{aligned}$$

Thus, because $\phi(gng^{-1}$ maps to the identity of G', $gng^{-1} \in N$ and $N \trianglelefteq G$.

5 The Rubik's Cube Group

Most everyone is familiar with the Rubik's Cube. The cube Puzzle has been a treasures for some and a pain in the neck for most! However, did you know that this humble cube, paired with a few simple movements, constitutes a mathematical group? The traditional variation of the Rubik's Cube has six sides, each of a different color. Of course the cube is often manipulated such that the colors are jumbled and it is the task of the user to restore the cube to it's original state.

So how can we say that the puzzle is a group? Lets say that you were to label every individual square on the rubics cube with a number 1-54. Importantly the middle squares of each face are not allowed to move as the puzzle requires twisting the outer faces. Thus only 48 of the 54 faces permute. The set of these permutations is the set portion of our Rubik's Cube group. Think of any arrangement of the faces and you will have a member of our set. Secondly, we need an operation. We will call this operation $\square$ and designate it as composition of **cube moves**. Since every permutation of the Rubik's Cube is a combination of turns involved to get there from a completed cube, $\square$, our operation, is intertwined with each and every permutation. Meaning that if you have the cube facing you, $L\square R$ is turning the left face and then the right face 90°.

Lets look at some more hands on examples. Allow e to designate the making of no cube moves, and L to designate turning the left side of the cube clockwise 90°. What is L^4?

$$L^4 = L\Box L\Box L\Box L = e.$$

While this looks convoluted, all that it says is that if you turn the left face of the Rubik's Cube clockwise 360°, it is as if you never turned it at all.

What about the closure axiom we have been so concerned about? Lets consider two elements $g, g' \in G$. Remember that g and g' are some permutation of the Rubik's Cube. These permutations are made through using our cube moves. Lets give them names:
R = Right Side
L = Left Side
B = Back Side
F = Front Side
T = Top Side
U = Underside
Once again, a move such as $L\Box R\Box T$ designates a 90° turn of first the left, then right and finally the top face of the cube. Order matters. Back to our proof. Considering both g and g' we are interested to see if $g\Box g' = g''$, for some $g'' \in G$. We see that for any;

$$\begin{aligned} & g\Box g' \\ & = (a\Box b\Box ...\Box f)\Box(a'\Box b'\Box ...\Box e') \\ & = (a\Box ...\Box f\Box a'\Box ...\Box e'). \end{aligned}$$

Where the letters a-f represent an arbitrary side being rotated. For instance a might equal T as defined above. Since G is composed of all permutations of the Rubik's cube, our new permutation created by $g\Box g'$ is contained in the group G and the set is closed under $\Box$.

Since we have proved closure, if we go ahead and show that every element in G has an inverse, then we will have shown something very special about our group G. Lets prove that elements in G all have an inverse and then more will be revealed! Consider any element $g \in G$. Lets say that $g = (a\Box b\Box ...\Box e)$, where letters a–e each correspond to some arbitrary side that is being rotated. We observe that;

$$\begin{aligned} & g^{-1} \\ & = (a\Box b\Box ...\Box e)^{-1} \\ & = (e^{-1}\Box ...b^{-1}\Box a^{-1}). \end{aligned}$$

If we stop to consider that that a 90° turn on an arbitrary side can be reverse by simply turning that side back 90°, we see that any cube move has an inverse. Finally, since all cube moves have inverses, all elements in G have an inverse as they are merely composed of cube moves. Imagine mixing up a Rubik's cube and created a permutation g. The inverse, g^{-1}, would simply be reversing the cube moves from the last to the first to get back to the solved puzzle.

So, what have we proved about the Rubik's Cube group that is so special? If you recall from earlier that we must only show closure and that each element has an inverse to prove that a subset is a subgroup. Important to our discussion is that the Rubik's Cube group is a subset of a group named S_{48}. Without getting too bogged down in another group, S_{48} is the collection of all of the permutations of 48 objects. Remember that our Rubik's Cube has 54 faces but that it is only possible to manipulate 48 of them.

If our Rubik's Cube group G were the same as S_{48}, it would be analogous to taking off all of the stickers and rearranging them in any way. However, we are bound by our cube moves; a colored sticker on a corner can not be moved to a non corner piece. Therefore all of the permutations of the Rubik's Cube group are contained in S_{48}. Because of this containment and the proof of our two axioms, we have shown that the set of Rubik's Cube permutations under the composition of cube moves is a group.

6 A Farewell to Groups?

A common and unfortunate question amongst students of math is often, "when will we use this?" Maybe the real question should be, "Where can I find this?" Sometimes you can hold math in your hand and not even know it. That was my intention when showing you the Rubik's Cube group. I know that you may or may not have been interested in everything in this writing. However, if at some point while reading you thought, "Wow, cool!" – then my job here is done. It has been a pleasure writing this paper. I hope that is has given you a greater appreciation for the beauty of mathematics.