Math Circles - Group Theory

Tyrone Ghaswala - ty.ghaswala@gmail.com

18th February 2015

"We need a super-mathematics in which the operations are as unknown as the quantities they operate on, and a super-mathematician who does not know what he is doing when he performs these operations. Such a super-mathematics is the Theory of Groups."
- Sir Arthur Stanley Eddington

Subgroups Generated by an Element

Before we move on, we will look at this very special kind of subgroup, which will shed a bit more light on our definition of the order of an element.

Let's look at an example, $(\mathbb{Z}_{15}, +)$, and let's consider the element 6 in this group. Similar to how we explored the subgroups of $\mathbb{Z}_6$ above, if we want 6 to be in our subgroup, $6+6$ had better be in there, and $6+6+6$, and so on. If we just take all elements in $\mathbb{Z}_{15}$ that arise this way, we end up with

$$\{6, 12, 3, 9, 0\}.$$

A quick check will convince you that this in fact is a subgroup of $\mathbb{Z}_{15}$. Notice that we didn't even have to think about closure or making sure all the inverses were in there, it took care of itself!

Let's do another example, this time in $\mathcal{Q}_8$, and let's consider the element i. Taking all powers of i we end up with

$$\{i, -1, -i, 1\}$$

which again is a subgroup of $\mathcal{Q}_8$. Does this happen in general? Well to answer this question, we need to work out exactly what we're asking.

Suppose we're in a group G and we have some element a with finite order (that is, there exists an n such that $a^n = 3$). Then does $\{e, a, a^2, \ldots, a^{n-1}\}$ form a subgroup of G? Notice that we could keep taking powers, but we wouldn't get any new elements, since for example, $a^{n+k} = a^n a^k = ea^k = a^k$.

So, let's see if it's a group. Well, the identity is in there, and it is closed under the group operation since if I take any two powers of a, I get another power of a. That is, $a^k a^l = a^{k+l}$. So all we have to check is if all the inverses are in there, and with a bit of thought we can see that $(a^k)^{-1} = a^{n-k}$ since $a^k a^{n-k} = a^{k+n-k} = a^n = e$.

Such a subgroup is called the **subgroup generated by** a in G. What do you notice about the order of this subgroup, and the order of the element a? This should explain why we defined the order of an element in the weird way that we did.

Cosets

Throughout this little course, we have seen lots of examples of patterns that we don't know how to prove (or whether or not they are even true!). For example, we have seen time and time again

that it seems like the order of an element must divide the order of a group. Or that if a group has order 8, then any subgroups must have orders 1,2,4, or 8.

At this point we don't really know whether these kinds of things are true in general (although it feels like they are in our hearts). In order to prove such results, we need to introduce the notion of a coset.

As always, let's start with an example. We have seen before that the groups $(\mathbb{Z}, +)$ and $(\mathbb{Z}_n, +)$ are very similar in many ways (even though one is infinite and one has order n). For example, the addition seems to work exactly the same in both of them. Let's get a new perspective on $\mathbb{Z}_n$.

Once we've played around with $\mathbb{Z}_n$ enough, we realize that it doesn't really matter which number mod n we use to do any calculation. For example, in $\mathbb{Z}_7$ we have

$$22 + 11 = 33 \equiv 5 \mod 7 \quad \text{OR} \quad 22 + 11 \equiv 1 + 4 \equiv 5 \mod 7.$$

and it doesn't seem to matter whether or not I use 1 or 8 or 22 when referring to the element 1. In fact, we can even thing of the element 1 to be the collection of all the possible options!

Let's explore this last comment a little more. Take $\mathbb{Z}_4$ for example. The 4 elements can be viewed as the following 4 sets:

$$\begin{aligned}
\{\ldots, -8, -4, 0, 4, 8, \ldots\} &= 4\mathbb{Z} \\
\{\ldots, -7, -3, 1, 5, 9, \ldots\} &= 1 + 4\mathbb{Z} \\
\{\ldots, -6, -2, 2, 6, 10, \ldots\} &= 2 + 4\mathbb{Z} \\
\{\ldots, -5, -1, 3, 7, 11, \ldots\} &= 3 + 4\mathbb{Z}
\end{aligned}$$

Notice the first element, the one corresponding to 0, is sipmly the subgroup $4\mathbb{Z}$. The one corresponding to 1 is the set of elements in $4\mathbb{Z}$ with 1 added to it, which we denote $1 + 4\mathbb{Z}$, and so on. Notice that $2 + 4\mathbb{Z} = -2 + 4\mathbb{Z} = 6 + 4\mathbb{Z}$, that is these are all the same set of elements.

One thing to note here is that these 4 sets actually form a group. How does the operation work? Well, if you want to add say $1 + 4\mathbb{Z}$ to $2 + 4\mathbb{Z}$, you simply take two things in those sets and add them together. For example, take 5 in $1 + 4\mathbb{Z}$ and 10 in $2 + 4\mathbb{Z}$. Then $5 + 10 = 15$, and 15 is in $3 + 4\mathbb{Z}$. So $(1 + 4\mathbb{Z}) + (2 + 4\mathbb{Z}) = (3 + 4\mathbb{Z})$, which is what you'd hope was true! Even better, it doesn't matter which two elements you choose, the result is always the same. This is special to this situation and unfortunately will not be the case.

In this example, the sets $4\mathbb{Z}$, $1 + 4\mathbb{Z}$, $2 + 4\mathbb{Z}$ and $3 + 4\mathbb{Z}$ are called the **cosets** of the subgroup $4\mathbb{Z}$ in $\mathbb{Z}$. In fact any set of the form $a + 4\mathbb{Z}$ for some $a \in \mathbb{Z}$ is a coset of $4\mathbb{Z}$. You can think of cosets as "shifts" of the subroup by a. Notice that if $a \in 4\mathbb{Z}$, then $a + 4\mathbb{Z} = 4\mathbb{Z}$.

Let's look at another example, the group $(\{1, -1, i, -i\}, \times)$. Let H be the subgroup $\{1, -1\}$. We can now ask, what are the cosets of H in the group? Well, let's just write them all out. Remember, a coset is a set of the form $a \times H$ for some a in our group. We have

$$\begin{aligned}
1 \times H &= \{1, -1\} \\
-1 \times H &= \{-1, 1\} \\
i \times H &= \{i, -i\} \\
-i \times H &= \{-i, i\}
\end{aligned}$$

and these are all the cosets. Looking at these we see that there are only two cosets of H in our group, and they are given by $1 \times H = -1 \times H$ and $i \times H = -i \times H$.

For another example, let's look at the subgroup $H = \{0, 3, 6\}$ in $(\mathbb{Z}_9, +)$. With a bit of elbow grease we see there are only 3 cosets of H, given by

$$\{0, 3, 6\} = 0 + H = 3 + H = 6 + H$$
$$\{1, 4, 7\} = 1 + H = 4 + H = 7 + H$$
$$\{2, 5, 8\} = 2 + H = 5 + H = 8 + H.$$

There are some interesting things to notice about these last 2 examples. For example, every coset has the same size, and it seems like any two different cosets are disjoint, that is they have no elements in common.

With this in mind you can now do questions 1 to 6.

The Last Hurrah - Lagrange's Theorem

Lagrange's theorem is one of the most important and fundamental theorems in group theory, and since groups are so ubiquitous in mathematics, it may well be one of the most important theorems in mathematics. Here is the statement of the theorem, and the rest of the course is dedicated to proving it.

Theorem 1 (Lagrange's Theorem)**.** *Let G be a finite group and $H < G$ a subgroup. Then $|H|$ divides $|G|$.*

The proof we will go through here will take many steps, and the hard part is realising which steps to take. We will first go through an overview of the proof and then do the details.

The general idea of the proof is in question 5 on question sheet 3. Here it is:

5. Let G be a finite group and $H < G$ a subgroup.

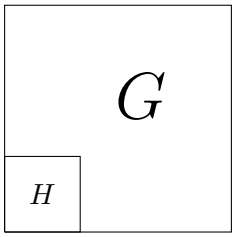
   (a) Prove that any two cosets of H have the same size.

   (b) Prove that every element of G belongs to a coset of H.

   (c) Prove that for any two cosets of H, they are either disjoint, or one is contained entirely in the other.

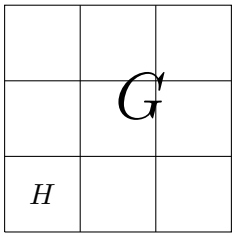
   Even if you didn't prove (a),(b), and (c), what can you deduce from these facts?

Let's talk a little bit about why proving these things is enough to prove Lagrange's theorem. Let's draw a little picture of our group G, with our subgroup H inside it.



If every element of g is in some coset, then we can completely cover G by cosets. Furthermore, if any two cosets are the same size, then if one is contained in the other, they are equal. Putting this together with the last property, we get that any two cosets are either equal, or are disjoint (that means they have no overlap).

Gathering all this information together means that we can completely cover our group G by the cosets of H, in such a way that no two cosets overlap and they all have the same size! If this is confusing, it means we can tile our group G as in the following image



where each little square is a coset of H. Since each square is the same size (each coset has the same size), then it is a little clearer now that the order of H must divide the order of G (and in the example image I've drawn, $9\,|H| = |G|$). So, take a bit of time to convince yourself that once we've answered question 5, we've proved Lagrange, and then we'll get down to business!

This proof is typical of proofs of difficult theorems throughout pure mathematics. We have a road map as to how to get to our theorem, but now we need to take the steps to get there. Each little step is called a lemma, and we will prove three lemmas which together will get us to our destination. In each lemma below, G is a finite group and H is a subgroup of G.

Lemma 2. *Any two cosets of H are the same size.*

Proof. Since G is a finite group, H is a finite group. Let

$$H = \{h_1, \ldots, h_k\}.$$

Then for any $a \in G$,

$$aH = \{ah_1, \ldots, ah_k\}.$$

It remains to prove that no two elements in the list $\{ah_1, \ldots, ah_k\}$ are the same. Suppose two are, then $ah_i = ah_j$ for some i and j. Then multiplying both sides on the left by a^{-1} we have $h_i = h_j$, and therefore we must have that $i = j$.

This shows us that both sets above have the same size, k. ■

Lemma 3. *Every element in G belongs to a coset of H.*

Proof. Since H is a group, $e \in H$. Given any element $g \in G$, $g = ge \in gH$ and therefore every element is in a coset of H. ■

Lemma 4. *Any two cosets of H are either disjoint, or one is contained in the other.*

Proof. Choose two cosets, aH and bH. If they are disjoint, we are done. If not, there exists some element in both, call it x.

Then $x = ah_1 = bh_2$ for some elements $h_1, h_2 \in H$. This tells us that $b^{-1}ah_1 = h_2$. Now we wish to show that aH is contained in bH. Let ah be an arbitrary element of aH. Then

$$ah = bb^{-1}ah_1h_1^{-1}h = bh_2h_1^{-1}h$$

and since $h_1, h_2, h \in H$, and H is a group, $h_2h_1^{-1}h \in H$. Therefore $ah \in bH$ and we can conclude $aH \subset bH$. ■

As discussed before, these lemmas are enough to conclude Lagrange's theorem! Since all we used in the proof was the definition of a group, Lagrange's theorem is true for absolutely every group we've talked about so far. This is the power of abstraction in mathematics.

Now that we have this hammer we can immediately conclude some amazing things. For example, any group with a prime order does not have any subgroups besides $\{e\}$ and itself.

Pretty neat hey?

Parting Ways

This is all for this course, but we have barely barely scratched the surface of this immensely deep and beautiful subject. There are so many more questions which have answers, and probably a lot more that need answers.

If you want to learn more about groups, pick up any textbook on group theory, and if you're just looking for some less technical light reading, check out the book "*Why Beauty Is Truth: A History of Symmetry*" by Ian Stewart. It's one of my favourites.

Enjoy!