Math Circles - Group Theory

Tyrone Ghaswala - ty.ghaswala@gmail.com

4th, 11th, 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

Introduction

Group theory is one of the most rich and accessible topics in all of pure mathematics. It is very easy to get your hands on groups, and the area is full of mystery and enjoyment.

Groups first had some serious influence in the early 1800s, when Évariste Galois, a young French mathematician, developed what is now known as Galois Theory. One of the things he developed and used groups to do was to prove something amazing about solving equations.

We all know that if I have a quadratic equation $ax^2 + bx + c = 0$ for some numbers a, b, and c, then the values of x which satisfy this equation are

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Here is a way to write down the solutions for any quadratic, using only roots, and the four operations, plus, minus, divide and times. It's natural to ask, what about solving $ax^3 + bx^2 + cx + d = 0$? Is there a solution for that? It turns out the answer is yes, and one of the answers (there are three in total) is given by

$$x = \sqrt[3]{\left(\frac{-b^3}{27a^3} + \frac{bc}{6a^2} - \frac{d}{2a}\right) + \sqrt{\left(\frac{-b^3}{27a^3} + \frac{bc}{6a^2} - \frac{d}{2a}\right)^2 + \left(\frac{c}{3a} - \frac{b^2}{9a^2}\right)^3}} + \sqrt[3]{\left(\frac{-b^3}{27a^3} + \frac{bc}{6a^2} - \frac{d}{2a}\right) - \sqrt{\left(\frac{-b^3}{27a^3} + \frac{bc}{6a^2} - \frac{d}{2a}\right)^2 + \left(\frac{c}{3a} - \frac{b^2}{9a^2}\right)^3}} - \frac{b}{3a}$$

This formula may be disgusting and unenlightening, but the important thing is that it exists! What about for a quartic equation (where the highest power of x that appears is 4)? Again, the answer is yes but the formula is an abomination! No one should ever have to use that formula to find roots, and making someone do that would be an effective form of torture.

At this point, it would be surprising if the answer was ever "no", but surprisingly, for a general quintic of the form $ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$, there is no analogue of the quadratic formula. This is an easy consequence of some of the results from Galois theory, which is built upon the sturdy and industrious foundation of group theory.

Today group theory is used in elliptic curve cryptography, areas of chemistry, and most notably physics as illustrated by this quote.

"The importance of group theory was emphasized very recently when some physicists using group theory predicted the existence of a particle that had never been observed before, and described the properties it should have. Later experiments proved that this particle really exists and has those properties."
- Irving Adler

The idea that something as abstract as group theory could actually predict the existence of a particle with certain properties is mind blowing. We don't really know why, but for some reason the universe truly seems to be written in the language of mathematics.

Above all of these applications, the most important reason for studying group theory for me is the indescribable aesthetic beauty that exists in the subject. It really is one of the most beautiful areas of pure mathematics.

The power of group theory lies in its abstraction, and its focus on structure. This all sounds very vague right now, but it will become clear as we start playing with some groups. Throughout this whole course, it will pay for you to have your eyes open and your brain switched on. There are lots of connections to be made, too many to mention, and you will only make them if you're constantly looking out for them. That feeling when you find a connection is one of the great rewards of pure mathematics.

All of this might make group theory seem like some amazingly large and inaccessible mathematical object, but that's not the case. In fact, you already know a whole bunch of examples of groups, so let's get right into it.

Cats

When a child learns what a cat is, they do not learn it by being told "a cat is a quadruped, typically with fur, that is usually evil and meows". Instead they just keep seeing cats until they have a complete understanding of what a cat is. We will take the same approach to learning about groups. I will not at first tell you what a group is, but for now we will just amass some examples.

Cat 1 - $(\mathbb{Z}, +)$

This group is made up of all the integers, and the only thing we have other than the set of whole numbers is the operation "+". So recall that

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

and notice that + is an operation that takes in two elements of $\mathbb{Z}$ and spits out another one. For example

$$\begin{aligned} 3 + 5 &= 8 \\ 5 + 3 &= 8 \\ 2 + (-1) &= 1 \\ 0 + 5 &= 5 \\ 0 + 6 &= 6 \\ (-10) + 0 &= -10 \\ 2 + (-2) &= 0. \end{aligned}$$

Notice that there appears to be something interesting going on with 0. It seems to have the property that

$$a + 0 = a = 0 + a$$

for every a in $\mathbb{Z}$. An element like this in a group will be called the **identity**. In this group, is there more than one such element?

Let's take a closer look at the last equation above, $2 + (-2) = 0$. 2 and -2 have an interesting relationship to each other. Notice that they add together to make the identity. In this case, we say -2 is the **inverse** of 2, and of course, 2 is the inverse of -2. In general, an inverse of an element a, is another element b such that $ab = e$ where e is the identity element.

Cat 2 - $(\mathbb{Q}, +)$

Here is another group, all the rational numbers $\mathbb{Q}$ under addition. Similar to the case above, if you add two rational numbers together you get another rational number. Furthermore, the identity again is given by 0.

Cat 3 - $(\mathbb{Q} \setminus \{0\}, \times)$

Now things get a little more interesting. Let's look at the group given by taking all the rational numbers *except for* 0, and this time only being able to multiply them together. The first thing to notice here is that if you take any two non-zero rational numbers and multiply them together, you end up with another rational number, so that's certainly a good thing.

We can again ask, what element in $\mathbb{Q} \setminus \{0\}$ is the identity? Well, whatever the identity is, it better have the property that multiplying any other number by it doesn't change that other number. With a bit of thought we can convince ourselves that the identity here is given by $\frac{1}{1}$ since

$$\frac{1}{1} \cdot \frac{a}{b} = \frac{a}{b} = \frac{a}{b} \cdot \frac{1}{1}.$$

So, if 1 (we will just write it like this instead of $\frac{1}{1}$ from now on) is the identity, what do inverses look like? Well, as above, the inverse of, say $\frac{3}{5}$ is some element in $\mathbb{Q} \setminus \{0\}$, call it $\left(\frac{3}{5}\right)^{-1}$, such that $\frac{3}{5} \cdot \left(\frac{3}{5}\right)^{-1} = 1$. Again, a bit of thought and elbow grease, and you can convince yourself that $\left(\frac{3}{5}\right)^{-1} = \frac{5}{3}$. See if you can justify to yourself why this is the case!

In general, for any element $\frac{a}{b}$ in $\mathbb{Q} \setminus \{0\}$, we see that under the operation of multiplication, $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$, which should explain to you why you were always taught that the inverse of $\frac{7}{2}$ is $\frac{2}{7}$.

Cat 4 - $(\{1, -1\}, \times)$

Now things get a little interesting. So far I have only given you examples of groups that we are familiar with, and all of them have been infinite. Now, let's look at the group where the only elements are 1 and -1, and the operation is multiplication. Let's do something different here, and draw out a **multiplication table**.

$\times$	1	-1
1	1	-1
-1	-1	1

Just by looking at this table, can you find the identity element? What about the inverses of both the elements?

Cat 5 - $(\{1, -1, i, -i\}, \times)$

It just keeps getting more and more interesting! I will just tell you how the multiplication works here and you will investigate this group in the exercises.

The i in the group above is the usual i from complex numbers (for those who are familiar with such things). For those who aren't, here's all you need to know.

In all your calculations, just treat i as a variable (like x), except wherever you see i^2, you replace it with -1. For example,

$$i \cdot (-i) = -i^2 = 1 \quad \text{and} \quad -1 \cdot i = -i.$$

Before I introduce you to any more cats, we first have to build up some background in clock arithmetic.

Clock Arithmetic

We are all familiar with number systems (whatever they are), say for example, the real numbers $\mathbb{R}$, or the rational numbers $\mathbb{Q}$, or the integers $\mathbb{Z}$. What all of these things have in common is not only that we're quite familiar with them, but that if you take any two things in one of these and multiply or add them together, you get another member of the number system. We might ask ourselves, what else could we consider?

Well that's simple, a clock of course!

Consider a clock with seven numbers, 0 through 6, with the 0 at the top. What we're going to do now, is to try to imitate arithmetic operations on this clock. We will call this clock *the integers modulo 7.* We denote it $\mathbb{Z}_7$ and it consists of the seven elements

$$\mathbb{Z}_7 := \{0, 1, 2, 3, 4, 5, 6\}.$$

But how do we do math in $\mathbb{Z}_7$? Well, kind of as you would expect to do math on a clock. For example,

$$\begin{aligned} 3 + 4 &= 0 \mod 7 \\ 1 + 2 &= 3 \mod 7 \\ 5 + 6 &= 4 \mod 7. \end{aligned}$$

So addition is just what you would do on a clock! So what is $-3 \mod 7$? Well -3 does not live in $\mathbb{Z}_7$ (since it's not one of 0,1,2,3,4,5 or 6), so which element is it? Whatever it is, call it Bob, it better have the property that $\text{Bob} + 3 = 0 \mod 7$. Therefore we have

$$-3 = 4 \mod 7.$$

Alternatively, we could just count backwards around the clock, either way will work and no harm will come to you! Let's do some more examples. What about 22 + 11? Well we have

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

Look at that, it doesn't seem to matter if we convert 22 and 11 to mod 7 before or after doing the addition. It turns out that this is always the case. It doesn't matter when you reduce things to live inside $\mathbb{Z}_7$, no harm will come to you.

Ok, so we've dealt with addition and subtraction (since subtraction doesn't really exist, it's just adding by negative numbers), but what about multiplication and division? Well multiplication will work as we expect. Given two numbers, multiply them together and then keep subtracting (or adding) multiples of 7 until you end up in $\mathbb{Z}_7$. Piece of cake! For example

$$\begin{aligned} 3\cdot 4 &= 5 \mod 7\\ 5\cdot 3 &= 1 \mod 7\\ 2\cdot 3 &= 6 \mod 7. \end{aligned}$$

So, what about division or inverses? What is $3^{-1} \mod 7$? Well, let's think about it for a moment. The element that equals 3^{-1}, whatever it is, call it Jenny, had better have the property that $(\text{Jenny})\cdot 3 = 1 \mod 7$. Well, since $3\cdot 5 = 1 \mod 7$, and $2\cdot 4 = 1 \mod 7$, we see

$$3^{-1} = 5 \mod 7 \quad \text{and} \quad 2^{-1} = 4 \mod 7.$$

Let's draw up a table of inverses for $\mathbb{Z}_7$.

x	0	1	2	3	4	5	6
x^{-1}	$*$	1	4	5	2	3	6

Notice here that every non-zero element appears exactly once in both rows, and since nothing multiplies by 0 to be 1, we leave that entry out.

Let's shift our attention now to $\mathbb{Z}_4$. So this is the clock with only $\{0,1,2,3\}$, with 0 at the top. Using the same idea as above we see $1+2=3 \mod 4$, $2\cdot 3 = 2 \mod 4$ and $-1 = 3 \mod 4$. Let's draw up a table of inverses for $\mathbb{Z}_4$.

x	0	1	2	3
x^{-1}	$*$	1	$*$	3

This is interesting, it appears that 2^{-1} does not exist, that is 2 does not have an inverse. You might ask how we know this. Well, if 2 has an inverse, it better be one of $\{0,1,2,3\}$, so let's just check them.

$$2\cdot 0 = 0 \mod 4, \quad 2\cdot 1 = 2 \mod 4, \quad 2\cdot 2 = 0 \mod 4, \quad \text{and} \quad 2\cdot 3 = 2 \mod 4.$$

Since none of these were $1 \mod 4$, we see that 2 does not have an inverse. Interesting. We must now make the following definition.

Definition. A number x in $\mathbb{Z}_n$ is called a **unit** in $\mathbb{Z}_n$ if x^{-1} exists. The set of all units in $\mathbb{Z}_n$ will be denoted by $\mathbb{Z}_n^*$.

So, for example, $\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$, and $\mathbb{Z}_4^* = \{1,3\}$. Let's get back to groups now.

More Cats

It turns out that modular arithmetic is an important source of examples of groups for us, and we get two different infinite families of groups from these clocks.

Cat 6 - $(\mathbb{Z}_n, +)$

Our first family of examples are the integers mod n under addition. For example, $(\mathbb{Z}_4, +)$ has 4 elements, $\{0, 1, 2, 3\}$ and addition works the same way it always has! For example,

$$-1 = 3 \quad \text{and} \quad 2 + 3 = 1.$$

From here on in there might be times where I just ignore the "mod 4" part of the equation, especially when it is clear what group we are working in. In this group, what is the identity? What is the inverse of 1? Remember here that "inverse" means the inverse in this particular group. Hint: it's not so different to $(\mathbb{Z}, +)$.

Cat 7 - $(\mathbb{Z}_n^*, \times)$

Our second family of examples comes from just looking at the units in $\mathbb{Z}_n$, which recall we denote by $\mathbb{Z}_n^*$. Remember the units are all the things which have an inverse (in the sense of multiplication). So, for example, $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$, and $\mathbb{Z}_4^* = \{1, 3\}$.

Again, we can ask the usual questions, what is the inverse in $\mathbb{Z}_7^*$? It better be in $\{1, 2, 3, 4, 5, 6\}$. What is the inverse of 3?

Before we move on, let's draw out a multiplication table for $(\mathbb{Z}_4^*, \times)$. Remember here that our only operation is multiplication, there's no addition to be seen!

×	1	3
1	1	3
3	3	1

Well well, this looks familiar. Remember what we said at the beginning, stay switched on and be constantly on the lookout for new connections!

Orders

We almost are ready to dive in to the question sheet, but first we need to talk about the order of a group and the order of an element.

Definition. The **order of a group** is the number of elements in that group.

Easy! For example, $|\mathbb{Z}_4| = 4$, and $|\mathbb{Z}_4^*| = 2$ since $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ and $\mathbb{Z}_4^* = \{1, 3\}$.

The order of an element is a little more subtle, so in order to define it, let's do some examples.

Consider the group $(\mathbb{Z}_4, +)$. Let's draw out what we will call a **power table** for $\mathbb{Z}_4$. Here's how it works, down the first column you write all the elements of $\mathbb{Z}_4$, and across the top row you list the numbers from 1 to however large you want to go. The entry for the row corresponding to 3 in $\mathbb{Z}_4$ and the column 4 will be what you get when you do $3 + 3 + 3 + 3$ in $\mathbb{Z}_4$. Convince yourself that the following table has been filled in correctly.

+	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0
1	1	2	3	0	1	2	3	0
2	2	0	2	0	2	0	2	0
3	3	2	1	0	3	2	1	0

Let's now draw out a power table for $(\mathbb{Z}_7^*, \times)$. Remember here that the operation is ×, so the table is

$\times$	1	2	3	4	5	6	7	8
1	1	1	1	1	1	1	1	1
2	2	4	1	2	4	1	2	4
3	3	2	6	4	5	1	3	2
4	4	2	1	4	2	1	4	2
5	5	4	6	2	3	1	5	4
6	6	1	6	1	6	1	6	1

These are very interesting tables, and you should stare at them and think very hard about all the patterns you see. In order to talk about the order of an element, we only need to focus on one pattern.

Definition. The **order of an element** a in a group G, which we will denote $|a|$, is the column in the power table in which the first identity element occurs in the row corresponding to a.

This is a mouthful, but let's do some examples. In $\mathbb{Z}_4$ above, since 0 is the identity, we have

$$\begin{aligned}|0| &= 1\\ |1| &= 4\\ |2| &= 2\\ |3| &= 4\end{aligned}$$

since those are the first columns in the rows corresponding to what's inside the $|\ |$ where a 0 appears. Similarly for $\mathbb{Z}_7^*$, since 1 is the identity we have

$$\begin{aligned}|1| &= 1\\ |2| &= 3\\ |3| &= 6\\ |4| &= 3\\ |5| &= 6\\ |6| &= 2.\end{aligned}$$

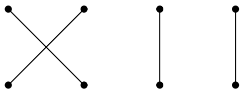
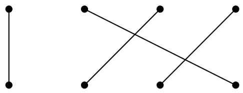
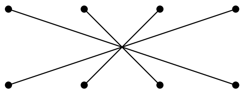
What do you notice about these numbers? What is $|\mathbb{Z}_7^*|$? If you think you notice anything, check it for other groups! You can now go on and do questions 1-5 on the first questions sheet.

Some different cats

So far we have a whole bunch of groups to play with and they're all familiar in some sense. Even if you haven't seen them before, they somehow come from our regular notion of a number, and our regular notion of multiplication and addition. Let's take a look at some other kinds of groups.

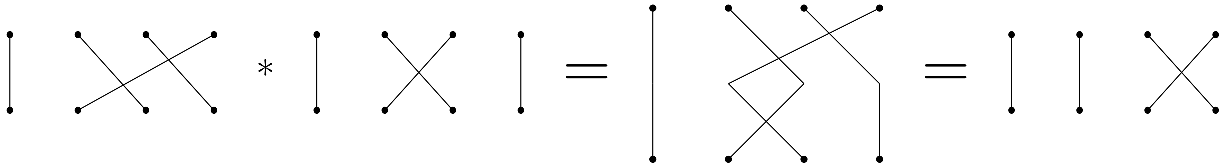
Cat 8 - $(\mathrm{Sym}(n), *)$

This group (sometimes called the permutation group) is a strange one, in the sense that the elements of the group aren't numbers, instead they are diagrams. Let's take Sym(4) for example. Here are some examples of elements.

 ,  and 

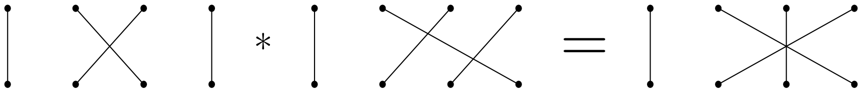
So the elements are diagrams which consist of two lines of n (in this case 4) dots, joined together by n lines. It is important that no dots are missed, and each one on top is matched to exactly one on the bottom.

So if this is a group, then there better be some sort of way to take two of these elements, combine them via some operation, and get another one. The operation is performed by taking the second diagram, putting it below the first one, and combining them. For example:



The key thing to notice here is that all we really care about are beginning and end points of the lines. One might now ask the usual questions, what is the identity? What are the inverses?

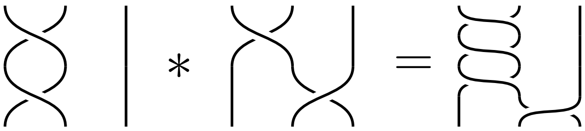
There is something fundamentally different about this group compared to all the groups we've seen so far. To see this let's look at the group operation we just performed, and let's do it in the opposite order.



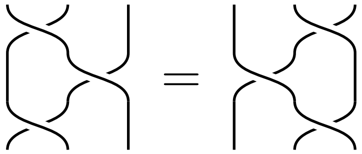
This gives us a different answer! This is strange, because it's the first time we've seen a group like this, that is a group with the property that $a * b \neq b * a$ in general.

Cat 9 - (Braid(n), $*$)

Let's take a look at another new group, this one's my personal favourite! The elements of this group are kind of like the ones above, except instead of straight lines, you imagine the dots on the top being joined to the dots on the bottom by a piece of string in 3-dimensional space. Here are some elements (which we call braids) in Braid(3), and an equation that demonstrates how the group operation works, which is much the same way as it does in (Sym(n), $*$).



One rule that needs mentioning, is that two braids are in fact the same braid if you can change one into the other, without moving the starting and ending points of the strings. For example,



since you can move the braid on the left to the braid on the right without moving the endpoints of the strings. Once again, we can ask ourselves what the identity is, and what the inverses are.

You now have enough to attack any question on sheet 1, the definition of the group (Poly(n), $*$) is coming below.

So what is a Group, Really?

So far we've seen a bunch of groups, but we still don't have a formal definition. You could argue that we have a pretty good feel for groups, so maybe a formal definition isn't necessary. Here are some things that we think a group should have:

- Groups need to have an operation.
- Groups need to have an identity element.
- Every element in a group needs to have an inverse.

Is that all? Or is there some other structure hiding in the background. We are now going to define a group formally, and we'll see that we weren't that far off. In the following definition and from here on in, the symbol $\in$ means "is an element of" or simply " in."

Definition (Definition of a group)**.** A **group** is a set G with an operation $\cdot$ such that

1. For any elements $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (this is called **associativity**).
2. There exists an element $e \in G$, which we call the **identity**, such that $a \cdot e = e \cdot a = a$ for all $a \in G$.
3. For all $a \in G$, there exists an element $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$. We call such an element the **inverse** of a.

Sometimes, if it is clear which group we're working in and what the operation is, we might ignore the operation and simply write $a \cdot b$ as ab.

At this point, we can look at this definition an it's not hard to believe that the groups we've seen so far are all in fact groups. However, a natural question arises: why in the world would we make such an abstract definition?

This is a perfectly valid question, and it is often definitions like this that turn people off pure mathematics. As we will see, there is incredible power in stripping off everything except for these bare bones. Now, if we prove something only using properties 1,2, and 3 of a group, then we have automatically proved it for anything that satisfies these properties. We've already seen an infinite number of groups, so if we prove something in this abstract setting, we've proved it for an infinite number of things. Amazing! We'll see this in all it's glory a little later.

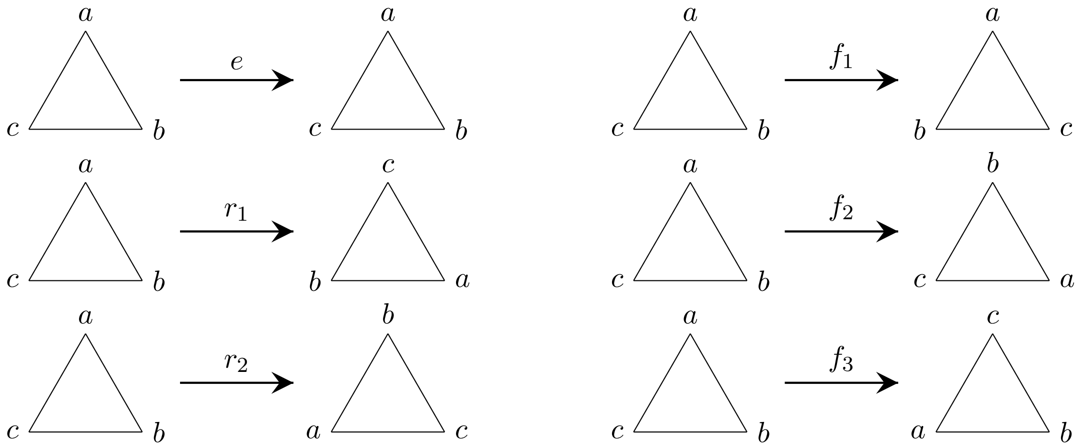
Even more cats!

Before we prove things in general, let's explore two more examples of groups. While we're going through these, it is important to check in your head that these are indeed a group by checking that the cat we're talking about satisfies properties 1,2, and 3 above.

Cat 10 - $(\text{Poly}(n), *)$

This group is the group of symmetries of a regular n-gon (a 3-gon is a triangle, a 4-gon a square etc). A symmetry of a triangle, say, is something I can do to a triangle when you're not looking, that when you look back, you can't tell I've done anything. For example, with a triangle, you can rotate 120 degrees around the centre, or you can flip it in three-dimensional space.

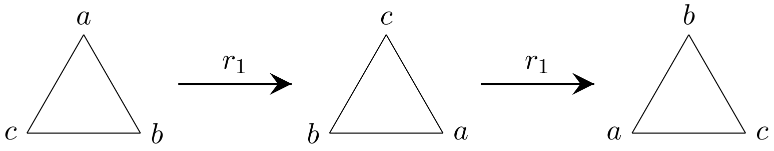
Let's write down all the elements in Poly(3). Below, the labels on the corners of the triangle aren't really there, they are just there for our benefit so we can keep track of what each symmetry does. This group has order 6, and here are the elements.



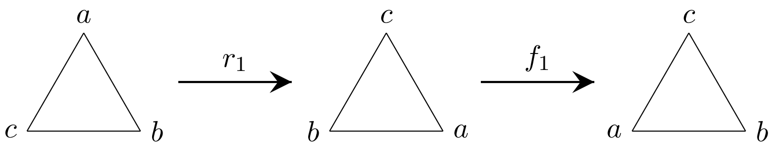
The symmetry e is simply the do nothing symmetry. Keep the triangle as is. The second symmetry, r_1 is a clockwise rotation around the center of the triangle by 120 degrees. The symmetry f_1 is obtained by flipping around the vertical axis. See if you can figure out how you get the rest of them, and convince yourself that these are all the possible symmetries of a triangle.

So, these 6 symmetries are our group elements, so how does the operation work? Well, whatever the operation is, it better take in two symmetries and spit out another one. It is defined in the only way you reasonably can, if you have two symmetries, create another one by composition. That is, do one and then the other!

For example, let's look at $r_1 * r_1$. If we do r_1 and then do r_1 again, we get



which is the same symmetry as r_2. So we have $r_1 * r_1 = r_2$. Let's see another example. Performing r_1 then f_1 we see



which is f_3, so $r_1 * f_1 = f_3$. Now that we know the formal definition of a group, we can ask whether or not this is a group. If so, what is the identity element? What are the inverses of all the elements?

Cat 11 - $(\mathcal{Q}_8, \cdot)$

This next group is called the quaternions. Quaternions are extremely important in physics, and play an important role in advanced algebra. We'll just be looking at them as groups (unfortunately).

The elements of the quaternions are $\mathcal{Q}_8 = \{1, -1, i, -i, j, -j, k, -k\}$, so $|\mathcal{Q}_8| = 8$. How does the operation work? Well, the first four elements should look familiar to you, where i is that special thing from the complex numbers that has the property $i^2 = -1$. The multiplication in $\mathcal{Q}_8$ is defined similarly to cat 5: treat i, j, and k has variables, except with the following rules.

$$i^2 = j^2 = k^2 = -1 \quad \text{and} \quad ij = k.$$

From these rules, and with a bit of ingenuity, we can work out what all the other multiplications give us. For example, let's try to work out what ji is. Well,

$$jik = jiij = -jj = -(-1) = 1.$$

We also have $(-k)k = 1$, so $(-k)k = jik$. Since we're in a group k has an inverse (it's $-k$, but let's pretend we don't know that). Multiplying on the right by k^{-1} we get

$$(-k)kk^{-1} = jikk^{-1} \implies -k = ji$$

so $ji = -k$. One of the exercise on sheet two is to draw out the multiplication table, which is an important exercise to understand this group.

As an aside, note here that $ij = -ji$, which is a similar property to a cross product in $\mathbb{R}^3$ as a vector space. This is not a coincidence, and it turns out that the existence of the quaternions is responsible for the existence of a cross product in $\mathbb{R}^3$. As a fun fact, the only other cross product that exists is in $\mathbb{R}^7$, and it corresponds to the existence of something called the octonions (which don't even form a group, but instead form some other algebraic structure).

Creating new cats from old ones - Direct products

Here is a way we can take two groups and create a new one, it's called a direct product. We'll first do an example which will indicate how it's defined in general.

Take for example, $(\mathbb{Z}_7^*, \times)$ and $(\mathbb{Z}_4, +)$. Then we can define the direct product of these two groups, and denote it $(\mathbb{Z}_7^* \times \mathbb{Z}_4, \cdot)$, or simply $\mathbb{Z}_7^* \times \mathbb{Z}_4$.

The elements of this group are of the form (a, b) where $a \in \mathbb{Z}_7^*$ and $b \in \mathbb{Z}_4$. Given two such elements, our group operation is performed in the most natural way possible, by just performing the old group operations in each of the coordinates. For example, $(4, 2)$ and $(3, 1)$ are in this group, where the first coordinates are in $\mathbb{Z}_7^*$ and the second are in $\mathbb{Z}_4$. Then the group operation will be performed as follows.

$$(4, 2) \cdot (3, 1) = (4 \times 3, 2 + 1) = (5, 3)$$

where the $\times$ is from $(\mathbb{Z}_7^*, \times)$ and the $+$ is from $(\mathbb{Z}_4, +)$.

In general we define the direct product of two groups $G \times H$ as you would expect. The elements are of the form (g, h) where $g \in G$ and $h \in H$, and the operation is given by $(g_1, h_1) \cdot (g_2, h_2) = (g_1 \bullet g_2, h_1 * h_2)$ where $\bullet$ is the operation in G, and $*$ is the operation in H.

Once again, we can ask the same age old questions: what is the identity, and what do the inverses look like?

What is True for All Groups?

So a small while ago, we defined what a group was in general, with the promise of reaping the rewards of this seemingly unnecessary abstraction. Here we will see one simple, but powerful result.

Theorem 1. *Say we are in a group. If $ab = ac$, then $b = c$.*

Proof. Since every element has an inverse a^{-1} exists. Multiplying on the left by a^{-1} we get

$$\begin{aligned} ab &= ac \\ \Rightarrow \quad a^{-1}(ab) &= a^{-1}(ac) \\ \Rightarrow \quad (a^{-1}a)b &= (a^{-1}a)c \\ \Rightarrow \quad eb &= ec \\ \Rightarrow \quad b &= c \end{aligned}$$

where the second step was possible by property 1 of being a group, the third step used the existence of inverses, and the fourth step used the existence and properties of the identity. This completes the proof. ■

One thing to note about this is that a proof is simply an argument which cannot be refuted about why something is true. Nothing more, nothing less.

So, as we mentioned before, since we only used the properties in the definition of a group, this theorem will be true for all groups, which is pretty amazing if you think about it.

At first glance, this result seems pretty boring, but let's explore one consequence in particular. Let's look at the multiplication table for a group, say $(\mathbb{Z}_3, +)$.

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Notice that every row and every column has all the elements in it. This is not a coincidence and is a direct consequence of the theorem we just proved. If one row had two entries which were the same, that would imply some element a and two others b and c where $ab = ac$ but $b \neq c$, which is simply not possible in a group (as we so fantastically showed).

In other words, filling out the multiplication table for a group is a little like solving a sudoku. Let's see what we can get out of this fact.

What Groups Can Exist?

Let's begin answering this question, first for groups of order 2. Well, in a group with 2 elements, one of them had better be the identity, so let's call our elements $\{e, a\}$. Then the first row and column of our multiplication table below are fixed by the property the identity has, leaving us only one option for the bottom right entry to ensure no entry is repeated in any column or row.

	e	a
e	e	a
a	a	e

The amazing thing about this is that it doesn't depend on the operation. Regardless of what the group is, if it has two elements, this is what its multiplication table must look like! For example, the multiplication table for $(\mathbb{Z}_6^*, \times)$ is

$\times$	1	5
1	1	5
5	5	1

and the multiplication table for $(\mathbb{Z}_2, +)$ is

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}.$$

So, if we only care about structure, there is only one group of order 2.

How about when $|G| = 3$? Well, let our elements be $\{e, a, b\}$, where e is the identity. Let's start filling out the table, as before, the first row and column are forced by the property the identity has.

$$\begin{array}{c|ccc} & e & a & b \\ \hline e & e & a & b \\ a & a & & \\ b & b & & \end{array}.$$

Now, if we put an e in the middle, then that forces a b to go in the middle right entry, which cannot happen because then two b's will appear in the right column. Therefore, the middle entry must be a b. From here we only have one choice for the rest of the entries and we get

$$\begin{array}{c|ccc} & e & a & b \\ \hline e & e & a & b \\ a & a & b & e \\ 2 & b & e & a \end{array}.$$

Compare this to the multiplication table for $(\mathbb{Z}_3, +)$ above. Notice anything? Since we only had one way we could possibly fill out this table, we can deduce that if we only care about structure, there is only one group of order 3.

This leads nicely into the following definition of groups being isomorphic, or essentially the same regardless of what we name the elements or what the operation is.

Definition. Two groups are **isomorphic** if you can relabel the elements of one with the elements of another in such a way as to (after possibly reordering the elements) make their multiplication tables look the same.

If we were in a spelling bee and I had to use isomorphic in a sentence, I would say that any two groups of order 3 are isomorphic.

Subgroups

Subgroups are what they sound like. They are subsets of groups, which when looked at by themselves, form a group when they use the same operation from the group they used to live in.

For example, let's look at the group $(\mathbb{Z}, +)$, and consider the subset $2\mathbb{Z} \subset \mathbb{Z}$, where

$$2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}.$$

We can ask the question, is $(2\mathbb{Z}, +)$ a group? Well, let's check. Does it have an identity? Yes, because it contains 0, which was the identity from the old group. Does everything have an inverse? Yup! Is it associative (does it satisfy property 1 of a group)? Definitely, because the bigger group was associative.

At this point you might think that we've provent that $2\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. However, we still need to check one more thing, and that is whether or not it is closed. What I mean by that is if

I take two things in $2\mathbb{Z}$ and add them together, do I stay in $2\mathbb{Z}$? Or, putting it another way, is $+$ really an operation on $2\mathbb{Z}$? A bit of thought will convince you that if you add two even numbers together, you get another even number, so $(2\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$.

Let's look at another subset of $\mathbb{Z}$. Consider the set $\{-4, 0, 4\}$. It has the identity, and everything has an inverse. However, $4 + 4$ is not in the set, so this does not form a subgroup.

Let's look at another example, $(\mathbb{Z}_6, +)$. We will now find all subgroups of $\mathbb{Z}_6$.

First, every subgroup has to have the identity, so let's start with that. Consider $\{0\}$. This has the identity, everything has an inverse, and if I take two things in there and add them together, I stay in there! Excellent, we found a subgroup.

Let's try to find another one. Let's take $\{0, 3\}$. Again, we check that this has an identity, $3 + 3 = 0$ so everything has an inverse, and it is closed under the operation, so this is another subgroup!

This time, let's look at $\{0, 2\}$. This has the identity, but the inverse of 2 isn't in there, so let's throw it in. Now we have $\{0, 2, 4\}$. A quick check will convince you that this is a subgroup as well.

Let's now start with $\{0, 5\}$. Not everything has an inverse, so let's throw in 1 to give us $\{0, 1, 5\}$. Now everything has an inverse, but $1 + 1$ is not in there. In fact, $1 + 1 + 1$ and $1 + 1 + 1 + 1$ are also not in there, so we better throw those in too. This leaves us with $\{0, 1, 2, 3, 4, 5\}$, which is the whole group (also a subgroup)!

You can keep looking, but once you exhaustively search all possibilities you will find that these are all the subgroups of $(\mathbb{Z}_6, +)$. They are $\{0\}$, $\{0, 3\}$, $\{0, 2, 4\}$, and $\mathbb{Z}_6$. As a curiosity, these groups have order $1, 2, 3$, and 6 respectively, all of which divide $6 = |\mathbb{Z}_6|$. Coincidence?

Let's explore these subgroups a little more, and see what they look like in the multiplication table. Let's draw it out for $(\mathbb{Z}_6, +)$.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Now let's see what each subgroup looks like in this table. The following tables are what the subgroups $\{0\}$,$\{0, 3\}$, and $\{0, 2, 4\}$ look like respectively living inside $\mathbb{Z}_6$.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

.

You can now do every question on sheet 2. Go nuts!

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:

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

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

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

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

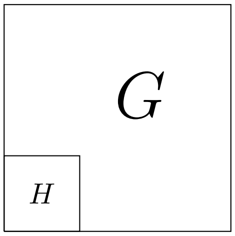
The proof we will go through here will take many steps, and the hard part is realising which steps to take. We will first go through an overview of the proof and then do the details.

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.

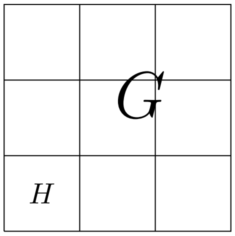
   Even if you didn't prove (a),(b), and (c), what can you deduce from these facts?

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 3. *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 4. *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 5. *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!