Math Circles - Group Theory

Tyrone Ghaswala - ty.ghaswala@gmail.com

4th 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!

$\times$	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 $\times$, 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

$$|0| = 1$$
$$|1| = 4$$
$$|2| = 2$$
$$|3| = 4$$

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

$$|1| = 1$$
$$|2| = 3$$
$$|3| = 6$$
$$|4| = 3$$
$$|5| = 6$$
$$|6| = 2.$$

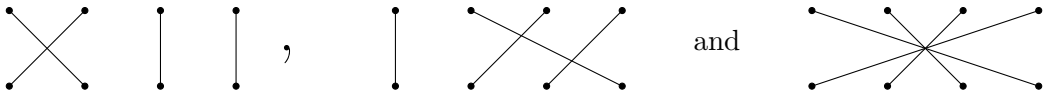
What do you notice about these numbers? What is $|\mathbb{Z}_7^*|$? If you think you notice anything, check it for other groups! You can now go on and do questions 1-5 on the first questions sheet.

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.

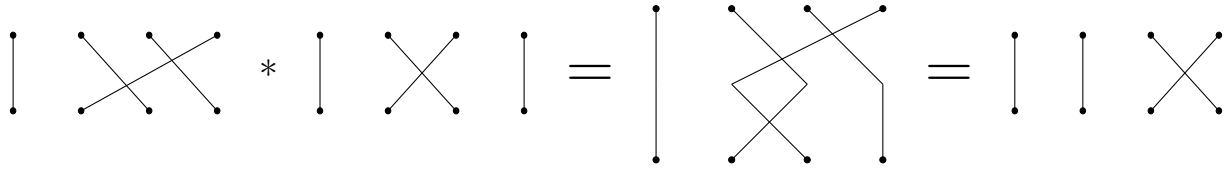
Cat 8 - $(\mathrm{Sym}(n), *)$

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.



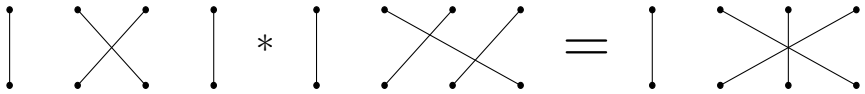
So the elements are diagrams which consist of two lines of n (in this case 4) dots, joined together by n lines. It is important that no dots are missed, and each one on top is matched to exactly one on the bottom.

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?

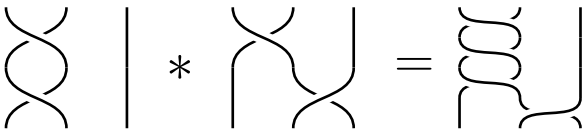
There is something fundamentally different about this group compared to all the groups we've seen so far. To see this let's look at the group operation we just performed, and let's do it in the opposite order.



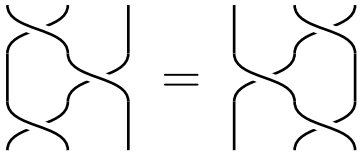
This gives us a different answer! This is strange, because it's the first time we've seen a group like this, that is a group with the property that $a * b \neq b * a$ in general.

Cat 9 - $(\text{Braid}(n), *)$

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 $(\text{Sym}(n), *)$.



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 $(\text{Poly}(n), *)$ is coming below.