Math Circles. Group Theory. Session 1.

Diana Carolina Castañeda Santos
dccastan@uwaterloo.ca
University of Waterloo

March 20, 2019

1 Introduction to Groups

One of the most important structures of study in pure mathematics are called *groups*. They are considered one of the first elements to study in the area of abstract algebra. Although they are abstract elements, once you are familiar with them and know how to identify them, playing with them and study properties on them becomes more natural and fun!

What we will do today is to have a look on different examples (you already know some of them), and we will conclude with the formal definition of what they are.

1. **Integers with addition.**

   We denote this group by $(\mathbb{Z}, +)$. The set of integers

   $$\mathbb{Z} = \{\cdots -3, -2, -1, 0, 1, 2, 3, \cdots\}$$

   with the usual addition of numbers. As a set, we are very familiar with it. Let's have a look on some properties. First, notice that "+" is an operation that takes two elements in $\mathbb{Z}$ and obtains another element in $\mathbb{Z}$. For example $1 + 50 = 51$, $0 + (-8) = -8$, or $20 + (-3) = 7$.

   Also, notice that the element 0 has an interesting property. For any number $a \in \mathbb{Z}$, $a + 0 = 0 + a = a$. An element with this property in a group is called the **identity**. Is there any other element in $\mathbb{Z}$ with this property?

Now, notice another interesting property. For any integer number a, there exists an integer b such that $a + b = 0$. What is that number b? How many elements satisfy this condition? Such element b in a group is called the **inverse** of a.

2. **Rational numbers with addition.**

   We denote this group by $(\mathbb{Q}, +)$. This example becomes more interesting. Can you find the identity element? How about the inverse of $\frac{2}{3}$? How about the inverse of 5? How about the inverse of a fraction $\frac{a}{b}$?

---

3. **Non-zero rational numbers with multiplication.**

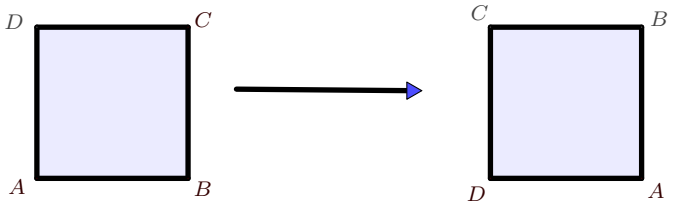
   We denote this group by $(\mathbb{Q} \setminus \{0\}, \cdot)$. Similarly as the previous example, if you add two rational numbers you get a rational number, the number 0 is the identity element, and every fraction has an inverse fraction.

4. The group $(\{1, -1, i, -i\}, \cdot)$. where i is the usual number i from complex numbers. If you are not familiar with them, that's ok. You can consider i as a variable with the property that $i^2 = 1$. Let's look at the operation of any pair of elements in this group in the following **multiplication table**.

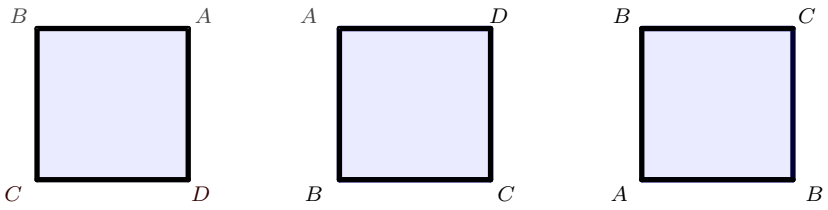
$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

5. **Dihedral Group of order** 8**.** This group is denoted by $(D_4, \cdot)$. Let us start

   by considering the symmetries of a square. To do it, imagine that we take a square region from the plane, we move it some way, and then we put it back into the space that it originally occupied. We want to study all the possible ways in which we can do this. Consider the square with labeled corners A, B, C, and D. One of the moves that we can do is to rotate the square 90° counterclockwise.



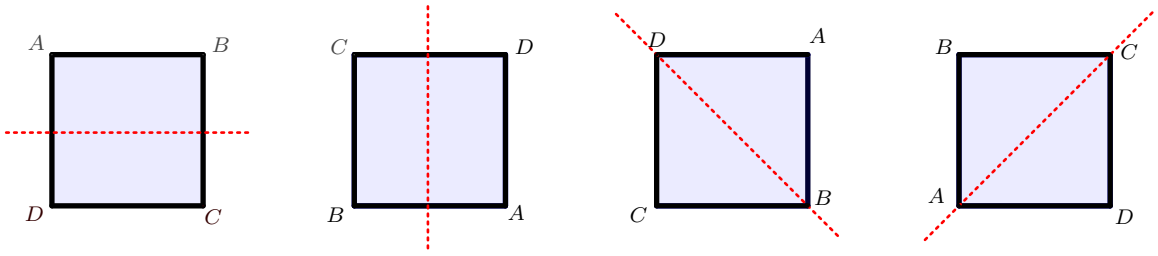
We can keep rotating the square and complete three more rotations counter-clockwise. Respectively 180°, 270°, and the 0° rotation.



Notice that all possible rotations are considered here. Even the clockwise rotations. Why?

Let's give these rotations a name. We will call the 90° rotation "R". The 180° rotation can be done by making two rotations of 90°, hence we will use the notation R^2 to represent the rotation of 180°. Similarly, we will use the notation R^3 to represent the 270° rotation, and finally we will use the notation e to refer to the 0° rotation.

There are other moves that we can perform with the square. For instance, we can flip it horizontally, vertically, and diagonally.



We denote the horizontal flip by H, the vertical flip by V, one of the diagonals

flip by D and the other by D'.

So far, we obtained eight different motions of the square. We claim that these are the only possible motions that can be made. Why?

Notice that we can compose two of these motions and get another motion. For instance, we can make the rotation R followed by the flip H to obtain the flip D. Let's register the composition of these eight moves in the following table:

$\cdot$	e	R	R^2	R^3	H	V	D	D'
e	e	R	R^2	R^3	H	V	D	D'
R	R							
R^2	R^2	R^3	e	R	V	H	D'	D
R^3	R^3	e	R	R^2	D	D'	V	H
H	H							
V	V	D'	H	D	R^2	e	R^3	R
D	D	V	D'	H	R^3	R	e	R^2
D'	D'	H	D	V	R	R^3	R^2	e

Complete the table and then discuss with a partner the following questions:

(a) What properties does only the element e satisfy?

_____

(b) By doing these compositions did we get any new motion different from the eight that we had?

_____

(c) Pick a motion A. Can you find a motion B such that $A \cdot B = e$? Can you find the inverse for each motion?

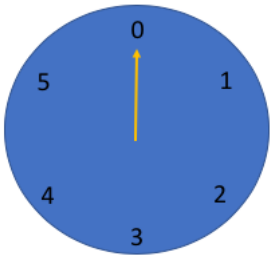
_____

(d) Does the order of the motions matter? Meaning that if we pick two motions A and B, is it true that $A \cdot B = B \cdot A$?

_____

6. We can generalize our last example. In fact we can take any regular polygon with n sides and construct the *Dihedral group of order* $2n$ and we denote it by D_n. We'll work on some of them in the problems session.

7. **Integers Modulo 6:** Imagine a clock with hours 0, 1, 2, 3, 4, 5. Clock arithmetic, or modular arithmetic consists on operating numbers in the clock.



We use operation "+" in the clock. For example $1 + 3 = 4$. we obtain this by moving the hour hand one hour followed by three hours. We will write this as $1 + 3 = 4 \mod 6$, to remind us that we are not using the addition of integers but rather the addition in the clock of 6 elements. Another examples are $2 + 4 = 0 \pmod 6$, $3 + 5 = 2 \pmod 6$.

You try:

$$\begin{aligned} 0+3 &= \_\_ \pmod 6 \\ 4+3 &= \_\_ \pmod 6 \\ 5+5 &= \_\_ \pmod 6 \\ 1+5+2+3 &= \_\_ \pmod 6 \end{aligned}$$

What is the identity? _____.

What is $-4 \pmod 6$? _____.

What is the inverse of 1? _____.

What is the inverse of 4? _____.

For a general element a, what is the inverse of a? _____.

This set is called the group of integers modulo 6 with addition, and it is denoted by $(\mathbb{Z}_6, +)$.

How about multiplication? Can we multiply numbers modulo 6?

Well, the answer is yes! We can also think on multiplication using the clock. Some examples are

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

So, we can see that multiplication in this set makes sense. Can we say that $(\mathbb{Z}_6, \cdot)$ is a candidate to be group? Well, to answer this, we need to find the identity and make sure that every element has a inverse. What can go wrong?

In the problems, we will see that this can be fixed and that for certain values of n, $(\mathbb{Z}_n \setminus \{0\}, \cdot)$ is a group!

8. **Integers modulo n with addition.** We can generalize the previous example of clock arithmetic to groups of order n. The group of integers modulo n is the set $\{0, 1, 2, 3, \cdots, n-1\}$ with the clock operation, and we denote this group by $\mathbb{Z}_n$. We will see more of these examples in the problem session.

Definition: Let G be a set. A binary operation G, is a function that assigns to each pair of ordered elements of G, an element in G.

Examples of binary operations:

- The operation of composition of motions in the set of motions of the square.
- The usual operation of addition of integers.
- The usual operation of multiplication of rational numbers.

Now we are ready to define what groups are...

Definition: Let G be a set with a binary operation $*$. We say that G is a group if it satisfies the following properties:

1. *Identity:* There exits and element $e \in G$ such that for all elements $a \in G$, $a * e = e * a = a$.
2. *Inverses:* For every element $a \in G$ we can find an element $b \in G$ (which we call the inverse of a) such that $a * b = b * a = e$.
3. *Associativity:* For every elements a, b, c in G, $a * (b * c) = (a * b) * c$.

   Additionally, we say the group is *Abelian* if for all elements a, b in G, $a*b = b*a$.

Of the examples of groups shown, which are abelian?
