Math Circles. Group Theory. Session 2.

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

March 27, 2019

1 More Examples and Properties Groups

Last time we saw a variety of examples of groups. This time, we will cover more examples and we will define what groups are. Before moving into the new material, last time we didn't talk about $(\mathbb{Z}_n, +)$ and $(\mathbb{Z}_p^*, \cdot)$. We will cover these examples first, and then we will continue with other examples. Check out the handout from previous lesson to study these groups.

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 $a^{-1} \in G$ (which we call the inverse of a) such that $a * a^{-1} = a^{-1} * a = e$.
3. *Associativity:* For any elements a, b, c in G, $a * (b * c) = (a * b) * c$.

Sometimes, when it is clear which group we are working in and what the operation is, we might ignore the operation and simply write $a \cdot b$ or ab.

We also said that abelian groups are those in which the order of the operation doesn't matter, or in other words, the operation is commutative ($ab = ba$). Those groups in which the order matters, are called *non-abelian* groups.

Before studying more examples and properties, let's define what we mean by order of a group and order of an element.

Definition: Let G be a group, the **order of** G is the number of elements in G, we denote the order of G by $|G|$.

Examples:

$$\begin{aligned} |(\mathbb{Z}_6^*, \cdot)| &= 2 \\ |(\mathbb{Z}_{10}, +)| &= 10 \\ |D_4| &= 8 \\ |D_3| &= 6 \\ |\{1, -1, i, -i\}| &= 4 \end{aligned}$$

Definition: Let $(G, *)$ be a group, the **order of an element** $a \in G$ is the smallest number n such that $\underbrace{a * a * \cdots * a}_{n} = e$, we denote the order of a by $|a|$. If that number doesn't exists, we say that a has infinite order.

Examples:

- Let $G = \mathbb{Z}_4$ with clock addition "+". To find the order of 2, we need to operate 2 with itself and find the smallest number of times that we need to add 2 to get the identity element (0). Since $2+2 = 4 = 0 \pmod 4$, we see that $|2| = 2$.

- In $(\mathbb{Z}_5, +)$, $|3| = 5$ because $3 + 3 + 3 + 3 + 3 = 15 = 0 \pmod 5$ and that is the smallest number of times that you have to add 3 to get 0.

- In D_4 the horizontal flip, denoted by H, satisfies that $H^2 = e$. Hence $|H| = 2$.

- In $(\mathbb{Z}, +)$, we know that any non-zero element added with itself won't be zero. Hence, every non-zero integer number has infinite order.

More examples of groups:

Now we will see another important class of groups, very useful in abstract algebra.

Symmetric group S_n: This is the group of permutations on a set with n elements and the operation is the composition. In this group, the elements are not numbers

but rather bijective functions on a set with n elements, for simplicity we choose the set $\{1, 2, \cdots, n\}$ and we study permutations of the numbers 1 to n.

Let's have a look on S_3. This is the set of permutations of the set $\{1, 2, 3\}$. How many permutations can we make of this set? Well, there are exactly 6 permutations:

$$1\ 2\ 3 \qquad 1\ 3\ 2 \qquad 2\ 1\ 3 \qquad 2\ 3\ 1 \qquad 3\ 1\ 2 \qquad 3\ 2\ 1$$

As we mentioned, we can see the permutations as functions and that helps us to describe the operation in this group by composing functions. For example, the permutation 2 3 1 can be represented as a function $f : \{1, 2, 3\} \longrightarrow \{1, 2, 3\}$ where $f(1) = 2$, $f(2) = 3$, and $f(3) = 1$. It is common to denote this permutation in the form:

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$$

Let's give names to the elements in this group:

$$\text{id} = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix} \quad (23) = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \quad (12) = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$$

$$(123) = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \quad (132) = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} \quad (13) = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$$

Now, to operate two permutations, we use the composition of functions. Recall that to compose two functions $f \circ g$, we first operate g and then f. So, let's calculate $(12) \cdot (123)$. First we use the permutation (123) and then we apply the permutation (12). Then, $(12) \cdot (123) = (23)$.

You try:

$$\begin{aligned} (23)(13) &= \_\_\_\_\_ \\ (123)(132) &= \_\_\_\_\_ \\ (12)(12) &= \_\_\_\_\_ \\ (12)(23)(123)(13) &= \_\_\_\_\_ \\ |(132)| &= \_\_\_\_\_ \end{aligned}$$

Is S_3 and abelian group? why?

_____

x	id	(12)	(13)	(23)	(123)	(132)
x^{-1}						

Find the inverse of each element in S_3.

In the problems we will study more properties of symmetric groups.
The next property holds for all groups:

Proposition: (Cancellation) Let G be a group and let $a, b, c \in G$. If $ac = bc$, then $a = b$.

Proof. Since G is a group, we know that the inverse of c, namely c^{-1} exists, so we can multiply by the right by c^{-1} and obtain

$$\begin{aligned} ac &= bc \\ (ac)(c^{-1}) &= (bc)(c^{-1}) \\ a(cc^{-1}) &= b(cc^{-1}) \\ a(e) &= b(e) \\ a &= b \end{aligned}$$

The third line is possible because of the property of associativity in G. The fourth line is due to the property of inverses in G and the last line is possible because of the property of the identity in G. This completes the proof. □

Another example of a group: $(\mathcal{Q}_8, \cdot)$. This is called the group of *quaternions*. This is an important group in physics and in advanced algebra. Here we will study it as a group. The elements in this group are $\{1, -1, i, j, k, -i, -j, -k\}$. So $|\mathcal{Q}_8| = 8$. The variables i, j, k interact with numbers as the case of complex numbers, and they have the properties $i^2 = j^2 = k^2 = -1$ and $ij = k$.

Just using these properties one can figure out all the elements in the multiplication table. For example, to find the product jk, we can use that $ijk = k^2 = -1 = i^2$, then $ijk = ii$ and using the cancellation property, we see that $jk = i$. In the problems we will find the multiplication table for this group.

2 Groups of all sizes.

So far we have seen examples of groups and some properties of them. But one important aspect of studying groups is to determine how many of them actually exist. Do we have groups of any order? More specifically, given a natural number n, can we

find groups of order n? How many distinct groups of that order exist?

What do you think? Discuss with a partner: Given a natural number n, can we find groups of order n?

_____.

Let's start studying this question by studying the number of elements in a group.

Can we have a group with one element? _____.

_____.

Now, let's study groups with two elements. Say that we want a group with elements $\{e, a\}$. Let's check out the multiplication table. We know how to operate with the identity element. Also remember that any element shows up in each column and each row exactly once. So the table is:

$\cdot$	e	a
e	e	a
a	a	

Well, this table is very familiar, we already know two groups with two elements. $(\mathbb{Z}_2, +)$ and $(\mathbb{Z}_4^*, \cdot)$. These two groups have different elements but their tables are the same. so if we care only about the structure, we say that these two groups are the same group. So there is only one group of order 2.

Let's study groups of order 3. Say that we have a group with three elements $\{e, a, b\}$. As before we try to complete the multiplication table. To do it, we use the properties of the identity element and the fact that we can't repeat elements in columns or rows. The table is given by:

$\cdot$	e	a	b
e	e	a	b
a	a		
b	b		

Notice that as before, we only have one possible way to complete this table, so if we care only about the structure, there is only one group of order 3. In fact we know a

group like this one $(\mathbb{Z}_3, +)$.

In the process of studying groups of order n for each $n \in \mathbb{N}$, the following definition became more clear. We were trying to say that two groups are the same if we look at their multiplication table and it looks pretty much the same up to relabel the elements.

Definition: Two groups are said to be **isomorphic** if one can relabel the elements of one group with the elements of the other in such a way that after relabel and reorder the multiplication tables are the same.

Examples:

- $(\mathbb{Z}_2, +)$ and $(\mathbb{Z}_6^*, \cdot)$ are isomorphic.

- $(\mathbb{Z}_8^*, \cdot)$ isomorphic to $\{1, -1, i, -i\}, \cdot)$