

Final Project Write-up

Charles Liu

Dr. Ben Clark

April 14th, 2025

General Overview of the Lesson Plan

To start the lesson and introduce a new topic to an audience of maybe not the highest mathematical background (high schoolers), I'm going to bring up things they are familiar with. For instance, they're not familiar with groups in a mathematical context, but they are familiar with it in a day-to-day context. I'm also going to relate other topics explained throughout with something real-life that they can understand, before I go to pure math.

Throughout the lesson, I'm going to ask questions and let students pause to think, so they can really grasp and digest the material. This will also help clarify misconceptions.

As I explain more, I'll become more technical and have less "training wheels" (with the real-life digestible examples) and stick more to mathematics.

In the end, I'll have students explain the concepts to me that they learned and relate it to something they know, so they really grasp the content.

Layout (linked for convenience):

- Slide 1: Title
- [Slide 2 Introduction](#)
- [Slide 3: Binary Operations](#)
- [Slide 4-5 Groups](#)
- [Slide 6-8: Group Properties \(Associativity, Identity, Inverse\)](#)
- [Slide 9: Order of a Group](#)
- [Slide 10: Common Examples of Groups](#)
- [Slide 11: Order of an Element](#)
- [Slide 12-13: Understanding Orders of Elements Examples: Suika Game and Real Mathematical Groups](#)

- Slide 14-15: Subgroups
 - Slide 16: Two-step Subgroup Test
 - Slide 17: One-step Subgroup Test
 - Slide 18-19: Centers
 - Slide 20: Centralizers
 - Slide 21: Recap
 - Slide 22: Thanks
-

Slide 2: Introduction

What comes to mind when you think of a *group*?

They might say something like a group of people, animals, fruits, etc. I'm then going to explain that yes, these are groups, and the reason they are groups is they all have something in common, they are all *related* in some way. All those things, in group theory, could be part of a *set*.

You can perform operations on a set. For instance, consider your example of [blank (let's say fruits for the purpose of this demo)]. I could add a fruit, take away a fruit, or even combine two fruits in a fruit basket.

Slide 3: Binary Operations

In group theory, if that operation follows some properties, it is called a *binary operation*. Take any two elements in our set, (let's call it G), and apply this operation between them, and we still get something in G . Since it relates G back onto itself, we also call this *closed*.

So for example, consider an example of fruit baskets. If I have two fruit baskets with fruits, and I combine them, I still have a fruit basket with fruits.

You can also consider integers under the binary operation addition. Take any two integers, (let's say 3 and 5), and add them together, we get 8, another integer.

Slide 4-8: Groups and Group Properties

But just having a binary operation isn't enough for a set in group theory to be classified as a group.

We need:

Associativity: $a(bc) = ab(c)$

We can do certain parts of the operation first as long as the entire arrangement/order is the same.

If I have an apple, a banana, and an orange, it doesn't matter if I put the apple first, and then the banana and orange together, or if I put the apple and banana together, then the orange. I'll still have an apple, banana, and orange in the basket in that order.

(I could bring in a basket and some fruits here for a live demonstration, or a pencil bag and some pens, anything works)

This is different from *commutativity*, where any order wouldn't matter. I could put the orange, banana, and apple in any order because I don't need that extra property.

When I add two numbers, I can add the first two first or the second two first.

Identity: $ae = ea = a$

We need to have an "identity" element that maps any element to itself.

Let's consider a set of some real "elements", fire, earth, air, and water. You could apply water to anything else and make it wet, earth to anything and make it soily, fire to anything and set it ablaze, but air won't change any element it acts on.

- When air acts on fire, its still fire.
- When air acts on earth, its still earth.
- When air acts on water, its still water
- When air acts on itself, its still air

So air is an "identity". We need to have this sort of element in our set in order for it to be called a group. We also usually label this element "e".

In the fruit basket situation, the identity element would be adding nothing. If I add nothing to a fruit basket with apples, it'll still be apples. If I add nothing to a fruit basket with bananas and oranges, it'll still be a basket with bananas and oranges

[Pause to think]

So what would the identity element for the integers under addition be?

Answer: 0.

0 added to any integer is just that integer.

Inverse: For any element $a \in G$, there exists an element $b \in G$ where $ab = e$.

We need something that can get you back to this "identity" element.

Again consider the fruit basket situation. Just as I could add a fruit into the basket, I can take one away. If I add one apple, I could take away one apple, and be left with nothing (the identity). So the inverse, in this case, would be taking away whatever was there.

[Pause to think]

So what would the inverse of all integers under addition be?

Answer: the negative of that integer. (e.g 1's inverse is -1)

[Pause to think]

Is the integers under multiplication a group? Why or why not. What about the rational numbers under multiplication?

Answer: No, the identity would need to be 1, but any integer besides 1 and -1 can't have an inverse that is also an integer (e.g. $2, 1/2$ isn't an integer). Also no, 0 doesn't have an inverse.

Slide 9: Order of a Group

For any group, we define their *order* (using the notation $|G|$) as the number of elements in that group.

For our previous "elements" example, there were 4 elements, so the order of that group would be 4.

Slide 10: Common Groups

Some common groups in group theory are:

- \mathbb{Z}
Integers under addition
- $\mathbb{Z}_n = \{0, 1, 2 \dots n\}$
Integers under addition modulus n
- \mathbb{Q}
Rational numbers under addition

[Pause to think]

What would the order of these be?

Answer:

Infinity, n , and infinity respectively.

[Pause to think]

Is \mathbb{Z}_n a subset of \mathbb{Z} ?

Answer:

Not quite. \mathbb{Z}_n represents the equivalence classes modulus n . So 1 isn't just 1, its the coset (we won't go over this term) all the integers that modulus n equal 1. In essence, they are two different objects.

Slide 11-13: Order of an Element

We can also have the *order* of an element. That's how many times I could apply the element onto itself using the group operation, and get the identity.

Let's break down what that means.

Let's think about a variation of the fruit basket game that you all know and love, the Suika game (high schoolers at PHS will understand this).



When you combine two watermelons, they go away (so you have enough space to keep playing). So in this case, the order of watermelons would be 2.

In a group of "elements", I could apply just apply air (the identity) and have air, so the order of air in that group is 1. Similarly, the order of any identity element in a group is 1.

[Pause to think]

So in my fruit basket situation, what would the order of an element, let's say adding a banana, be?

Answer: Infinity, because we can keep adding bananas to the basket (unless there's restrictions like the basket size).

[Pause to think]

So what would the order of 1 in \mathbb{Z}_8 be? What about 2 or 3.

Answer: 8, 4, 8 respectively.

1 is the standard generator, $\gcd(2, 8) = 4$, and $\gcd(3, 8) = 8$.

Slide 14-15: Subgroups

If a set H contained in G is also a group under G 's operation, then it is a *subgroup*.

We use \leq and $<$ to denote subgroups and proper subgroups respectively.

Proper subgroups means there's at least one element that's in the group, but not in the subgroup.

Consider our fruit baskets example. Adding/Taking away all types fruits is a group, but adding/taking away just apples would be a subgroup.

Slide 16: Two-step Subgroup Test

We can use the two step subgroup test to determine if a subset of group G is a subgroup.

Given $a, b \in H$ where H is a nonempty subset of G ,

1. $ab \in H$ - the operation is still closed
2. $a^{-1} \in H$ - we still have an inverse in the subgroup

It's important to not count out the fact that the subgroup still has to be *nonempty*! That's why it's really 3 parts.

[Pause to think]

Is $5\mathbb{Z}$ a subgroup of \mathbb{Z} ? What about $n\mathbb{Z}$ for arbitrary $n \in \mathbb{Z}$?

Answer:

Yes.

First, $5\mathbb{Z}$ is nonempty because it contains many elements, such as 5.

Take $x_1, x_2 \in \mathbb{Z}$. Consider $5x_1, 5x_2 \in 5\mathbb{Z}$.

1. $5x_1 + 5x_2 = 5(x_1 + x_2) \in 5\mathbb{Z}$

2. $5x_1 + 5(-x_1) = 0$, and 0 is the additive identity of \mathbb{Z} . Since $-x_1 \in \mathbb{Z}$, $-5x_1 \in 5\mathbb{Z}$, and the inverse exists and is in $5\mathbb{Z}$.

Similar for n .

Slide 17: One-step Subgroup test

We can condense the two-step test to one-step

Given $a, b \in H$ where H is a nonempty subset of G ,

1. $ab^{-1} \in H$ - the operation is still closed and the inverse is in H

[Pause to think]

Prove that $5\mathbb{Z}$ is a subgroup of \mathbb{Z} with the one-step subgroup test instead of the two-step.

$5\mathbb{Z}$ is nonempty, as it contains 5.

Take $x_1, x_2 \in \mathbb{Z}$. This means $5x_1, 5x_2 \in 5\mathbb{Z}$

1. $5x_1 - 5x_2 = 5(x_1 - x_2) \in 5\mathbb{Z}$

Slide 18-19: Centers

The center, $Z(G)$, is the subset of elements in group G where all elements in $Z(G)$ commute with every element in G .

That is,

$$Z(G) = \{a \in G \mid ax = xa \text{ for all } x \in G\}$$

Consider the group of all invertible two-by-two matrices, denoted $GL_2(n, \mathbb{R})$. The centralizer in this group is all diagonal matrices.

Proof:

$$\text{Take } A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(n, \mathbb{R}), D = \begin{bmatrix} e & 0 \\ 0 & f \end{bmatrix}$$

$$AD = DA = \begin{bmatrix} ae & bf \\ ce & df \end{bmatrix}$$

Slide 20: Centralizers

The centralizer, denoted $C(a)$, is the set of all elements in G that commute with a , which is also in G .

$$C(a) = \{g \in G \mid ag = ga\}$$

So for our previous matrix example, the centralizer of any non-diagonal matrix might be the set of all diagonal matrices, whereas the centralizer of a diagonal matrix might be the set of all non-diagonal matrices.

Slide 21: Recap

So we learned about a lot of things today. Ask the audience: "Who can tell me what a group is, and a real-life example of one?". "What about a subgroup?", etc. Have them explain what they just learned so it actually sticks.