Math Circle Worksheet
Groups

Wesley Hamilton

1 Groups

In this worksheet we'll introduce the concept of a group, one of the most fundamental objects in mathematics. We'll start with the definition of a group and work out some basic properties every group shares. Next we'll play around with a few examples, and nonexamples, of groups. Finally, we'll prove a meatier theorem called Lagrange's theorem. This theorem will give us some insight into the kind of structures groups (and their subgroups) can have.

1.1 Definitions and Basic Properties

Informally, a *group* is a set of elements together with an identity element and a rule for combining two elements.

This isn't a rigorous definition, but it does give the general idea of what a group is.

So what is a group?

Definition. *A* ***group*** *is a set G together with a rule (also called a group operation) $\star$ for combining elements, and we will write this group as $(G, \star)$. The rule $\star$ must satisfy four properties:*

i. *if a and b are in G, then $a \star b$ is also in G (we say that G is* ***closed*** *under $\star$);*

ii. *if a, b, and c are all in G, then*

$$(a \star b) \star c = a \star (b \star c).$$

(We say that $\star$ is ***associative****);*

iii. *there exists an identity element e that satisfies*

$$e \star a = a \star e = a$$

for any element a in G;

iv. *for any element a in G, there exists an inverse element b such that*

$$a \star b = b \star a = e.$$

A very familiar example is the set of integers $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$ together with the group operation of addition $+$, the group $(\mathbb{Z}, +)$. To make sure, we check each of the properties that $+$ must satisfy:

i. If n and m are any two integers, like $n = 17$ and $m = 29$, then

$$n + m = 17 + 29 = 46,$$

and 46 is an integer. In general the sum of two integers is an integer, so the set G is closed under addition.

ii. If n, m and l are integers, then

$$(n + m) + l = n + m + l = n + (m + l).$$

Therefore $+$ is associative.

iii. The identity element of $(\mathbb{Z}, +)$ should be 0, so we make sure it satisfies everything an identity should satisfy: if n is any integer, then

$$n + 0 = 0 + n = n.$$

This tells us that 0 is indeed the identity of $(\mathbb{Z}, +)$.

iv. Finally, we need to show that every integer has an inverse. In this case, if n is an integer its inverse should be $-n$, and we check that indeed

$$n + (-n) = n - n = 0 = (-n) + n.$$

Since we've verified the four properties that the group operation addition must satisfy, we can conclude $(\mathbb{Z}, +)$ is a group. In other words, the integers under addition form a group.

1.2 Familiar Examples (and non-examples)

A few sets, together with a group operation, are given below. Decide if each is a group or not. If it is a group, what is the identity element and what does a typical inverse look like? If it isn't a group, what group operation property fails?

1. Let $\mathbb{N} = \{0, 1, 2, 3, ...\}$ be the set of non-negative integers, and let addition $+$ be the group operation.

2. Take the set $\mathbb{Z}$ of integers again, but this time let the group operation be multiplication $\times$.

3. Consider the set of rational numbers

$$\mathbb{Q} = \left\{ \frac{a}{b} : a, b \text{ are integers, and } a \text{ is non-zero} \right\}.$$

Let the group operation be the usual addition of rational numbers.

4. Let $\mathbb{Q}^*$ be the set of non-zero rational numbers, i.e.

$$\mathbb{Q}^* = \left\{ \frac{a}{b} \colon a, b \text{ are non-zero integers} \right\}.$$

   Let $\times$ be the standard multiplication of numbers.

5. Let $\mathbb{Q}$ be as above, this time with the group operation $\times$.

6. Let $\mathbb{Q}^*$ be as above, this time with the group operation $+$.

1.3 Some Fun Examples

For the first fun example imagine a soldier standing at attention facing you. There are three different things the soldier can do: stand still, which we'll write as s; turn right, which we'll write as r; turn left, which we'll write as l; turn around, which we'll write as t. The total collection of actions the soldier can do is $T = \{s, r, l, t\}$.

7. Is this collection of actions a group? Why?

8. What is the identity element?

9. For each non-identity action, what is the inverse?

10. What does the action $rlrtsl$ simplify to?

Another fun example is the "One Sock" group[1]. Suppose you're only wearing one sock, and you can do any of the following actions with the sock:

- n, where you don't do anything;
- c, where you take it off and put it on the other foot;
- i, where you take it off, turn it inside out, and then put it on the same foot;
- t, where you take it off, turn it inside out, and then put it on the other foot.

The total collection of actions you can do with the sock is then $S = \{n, c, i, t\}$.

11. Is the collection S a group?

12. What is the identity element?

13. What is the inverse of c?

14. What is the inverse of i? What about the inverse of t?

15. If the sock starts on your right foot, inside out, where will it end up after the action $itic$?

[1]This and the above example are from the book "A Decade of the Berkeley Math Circle."

Notice that both the Turning Soldier group and One Sock group have 4 elements.

16. Are the Turning Soldier and One Sock groups actually the same group? Why or why not?

Next imagine 12 people are standing in a circle, and suppose they are numbered $0, 1, 2, 3, ..., 11$. Person 0 picks up a ball and is only allowed to pass it to the person on their left, which we'll denote by $+1$. If we keep track of the person holding the ball then, if 0 passes it to their left, we write $0 + 1 = 1$, so the ball is now with person 1. Similarly if person 3 has the ball and they pass it to their left, then the ball gets passed to person $3 + 1 = 4$.

17. Who does person 11 pass the ball to? How would you express this mathematically?

18. Is there another familiar (everyday) object that behaves like this?

19. Suppose person 0 wanted to pass the ball to person 4. How would they do this? How would you express this mathematically?

This group is usually denoted $\mathbb{Z}_{12}$, and actually has the same group structure as clocks do!

20. Suppose we change the rule so that people can only pass the ball to the 2nd person on their left (so 0 can only pass to 2, 1 can only pass to 3, etc.). If 0 start with the ball, and people keep passing the ball to their left, what eventually happens? Does the ball get passed to everyone?

21. What if instead of passing the ball to the 2nd person, they're only allowed to pass it to the 4th person to their left (so 0 passes to 4, 1 passes to 4, etc.). What happens now? Does the ball get passed to everyone?

22. Finally, the ball is only allowed to get passed to the 5th person to the left. What happens in this case? Does the ball get passed to everyone now? Why or why not?

The last three problems dealt with the *orbit* of the ball, i.e. looking at what happens to the ball if you keep applying the rules over an over.

Suppose seven people get bored with this game, but everyone else wants to keep playing. A new circle gets formed with 5 people.

23. If the same rule is used at the end of the last game (passing it to the 5th person), then whoever starts with the ball gets to keep it forever (why?). If they go back to the rule where you can only pass it to the 2nd person on their left, what ends up happening?

24. Try this out with the remaining numbers: they're only allowed to pass the ball to the 1st, 3rd, or 4th person on their left. What patterns do you notice? Do some of these games look familiar?

In general, if you have n people in a circle people in a circle playing this game the group is written $\mathbb{Z}_n$. The group elements are the people numbered $0, ..., n$, and the group action is addition (person i passes the ball to the kth person on their left, so the ball ends up with person $i+k$). It's not exactly ordinary addition though, since in $\mathbb{Z}_{12}$ person 11 passes the ball to person 0. This is called modular arithmetic, or addition mod n.

25. We saw that the orbit of the ball in $\mathbb{Z}_{12}$ may or may not have been all of Z_{12}, depending on how much was added each time and who started with the ball. Adding 2 or 4 each time left some people out, whereas everyone was passed the ball if we added 5 each time. Why do you think this was the case?

26. The orbits of $5, 7$, and 11 will be all of $\mathbb{Z}_{12}$. Why?

27. The orbits of $2, 3, 4, 6, 8, 9$, and 10 will not be all of $\mathbb{Z}_{12}$. Why?

28. How many people are in each of the orbits from the last question? Why?

29. Suppose instead of 12 we have n people, and we add 3 each time. What does n have to be to ensure the orbit is all of $\mathbb{Z}_n$?

30. We're in $\mathbb{Z}_n$ again, but this time we add k each time, where k can be any integer. If the orbit is all of $\mathbb{Z}_n$, what can we say about the relation between k and n?