Group Theory I

Kevin Li

February 2022

1 Introduction

Definition 1. A **group** is a set G together with a binary operation $* : G \times G \to G$ which satisfies the following conditions (called **Group Axioms**):

1. For any $x, y, z \in G$, $(x * y) * z = x * (y * z)$ **(Associativity)**

2. There is an element $e \in G$ such that for any $g \in G$, $e * g = g = g * e$ **(Identity Element)**

3. For any $g \in G$ there is some $h \in G$ such that $g * h = e = h * g$. We usually denote such h by g^{-1} **(Inverse Element)**

Example 2. The most common binary operations are your usual addition, $+$, and multiplication, $*$. It is called a binary operation because it takes two inputs and returns one output (ex. $1 + 4 = 5$, $2 * 6 = 12$). For example, consider $(\mathbb{Z}, +)$. This is the set of integers with addition as the operation. To show this is a group, we have to show this pair satisfies the three conditions given above.

1. As in all of our experiences, the integers are associative. We can take this as a fact. For any $x, y, z \in \mathbb{Z}$, $(x + y) + z = x + (y + z)$. Usually, associativity will not be difficult to show

2. We need to find some element $e \in \mathbb{Z}$ such that for any $g \in \mathbb{Z}$, $e + g = g = g + e$. The element 0 fits such property, $0 + g = g = g + 0$

3. Now, let $g \in \mathbb{Z}$. We want some $h \in \mathbb{Z}$ such that $g + h = e = h + g$. Remember, we have found that $e = 0$. Thus, we want to find some h such that $g + h = 0 = h + g$. Since we have some g, if we pick $h = -g \in \mathbb{Z}$, then $g + (-g) = 0 = (-g) + g$

Problem 1. Show that $(\{-1, 1\}, *)$ is a group.

1. Check associativity: is $(x * y) * z = x * (y * z)$ for any $x, y, z \in \{-1, 1\}$? We know that $\{-1, 1\}$ is a subset of the integers $\mathbb{Z}$ and associativity of multiplication holds over the integers. What does this tell us about $\{-1, 1\}$?

Since the integers are associative, and $\{-1, 1\}$ is a subset of the integers, then it is also associative.

2. Find some element $e \in \{-1, 1\}$ such that $e * 1 = 1 = 1 * e$ and $e * (-1) = (-1) = (-1) * e$. Since $\{-1, 1\}$ only has two elements, we only have two choices for e. Find which one works.

You can check that $e = 1$ suffices in both cases.

3. Using the e found in part 2, find h_1 and h_{-1} such that $1 * h_1 = e = h_1 * 1$ and $(-1) * h_{-1} = e = h_{-1} * (-1)$

We have that $h_1 = 1$ as $1 * 1 = 1 = e$ and $h_{-1} = -1$ as $(-1) * (-1) = 1 = e$.

Problem 2. Show the following are not groups by finding which group axioms 1-3 do not hold:

1. $(\mathbb{N}, +)$

Axiom 2 does not hold. Suppose there exists $e \in \mathbb{N}$ such that for any $g \in \mathbb{N}$, $e + g = g = g + e$. Since $e \in \mathbb{N}$ we know that $e > 0$. Similarly for g, $g > 0$. Then it follows that $g + e > g$ which is a contradiction. So no such e can exist.

2. $(\mathbb{Z}, *)$

Axiom 3 does not hold. You can show that $e = 1$ satisfies the identity element. Then, for any $g \in \mathbb{Z}$, if g^{-1} exists we must have $g * g^{-1} = e = 1$. But for $g = 0$, $0 * g^{-1} = 0 \neq 1 = e$. So 0 has no inverse element.

Definition 3. Let $(G, *)$ be a group, and $H \subseteq G$. If $(H, *)$ satisfies the group axioms, we call H a **subgroup** of G, denoted $H \leq G$.

Definition 4. Recall the meaning of $\pmod n$ from previous worksheets. We know that for any integer $x \in \mathbb{Z}$, $x \equiv r \pmod n$ for some $r \in \{0, 1, \ldots, n-1\}$. Define the set $\mathbb{Z}/n$ as the set $\{0, 1, \ldots, n-1\}$ where every integer $x \in \mathbb{Z}$ is associated with r such that $x \equiv r \pmod n$ for some $r \in \{0, 1, \ldots, n-1\}$.

Problem 3. Consider $\mathbb{Z}/4 = \{0, 1, 2, 3\}$. Find the set of integers that are associated to each element. (Find the integers which are associated to 0. In other words, find all integers which are congruent to 0 $\pmod n$. Do the same for 1,2,3)

The integers congruent to 0 are $\{4n \mid n \in \mathbb{Z}\}$.
The integers congruent to 1 are $\{4n + 1 \mid n \in \mathbb{Z}\}$.
The integers congruent to 2 are $\{4n + 2 \mid n \in \mathbb{Z}\}$.
The integers congruent to 3 are $\{4n + 3 \mid n \in \mathbb{Z}\}$.

We often write $\mathbb{Z}/n = \{[0], [1], \ldots, [n-1]\}$ where $[k]$ is the set $x \in \mathbb{Z}$ where $x \equiv k \pmod n$. These are called **equivalence classes**.

Problem 4. Let $n \in \mathbb{N}$. Show that $(\mathbb{Z}/n, +)$ is a group.

1. Associativity holds
2. The identity element of the group is $e = 0$
3. The inverse element of any $g \in \mathbb{Z}$ is $n - g$. If $g = 0$, then $n - g = n \equiv 0$.

Definition 5. A **Cayley table** of a finite group $(G, *)$ is some $n \times n$ array where the entry (x, y) is equal to $x * y$ in G.

Example 6. Consider the group $(\{-1, 1\}, *)$ as in problem 1. The Cayley table for this group is:

*	1	-1
1	1	-1
-1	-1	1

Problem 5. Write out the Cayley table for the groups $(\mathbb{Z}/7, +)$ and $((\mathbb{Z}/7)\backslash\{0\}, *)$ (you don't have to show the second is a group...yet)

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

*	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Notice that if you switch the rows and the columns, the tables remain exactly the same.

Problem 6. The commanding officer of the famous 00 unit of the British intelligence service MI6 suspects that one of the seven 00 agents is a Russian mole. He hires you as a consultant to organize the following way for the 00 agents to spy on one another. Agent 001 spies on the agent spying on agent 002. Agent 002 spies on the agent spying on agent 003 and so on. Finally, agent 007 spies on the agent spying on agent 001. How would you achieve that? Try to solve the same problem with eight agents instead of seven.

For 7 agents use the cycle $1 \to 5 \to 2 \to 6 \to 3 \to 7 \to 4 \to 1$.
For 8 agents, it is not possible.

Definition 7. A group $(G, *)$ is called **abelian** if for any $x, y \in G$, $x * y = y * x$.

Definition 8. Let $(G, *)$ be a group. Then the **cyclic subgroup generated by g** is the set $\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$ where $g^k = g * g * \ldots * g$ (k g's) for $k \in \mathbb{N}$, g^{-k} is the inverse of g^k for $k \in \mathbb{N}$, and $g^0 = e$. G is called **cyclic** if $G = \langle g \rangle$ for some $g \in G$

Problem 7. Write out explicitly the elements of $\langle 2 \rangle$ in the group $(\mathbb{Z}, +)$

$\langle 2 \rangle = \{2 * n \mid n \in \mathbb{Z}\}$

Problem 8. Is $(\mathbb{Z}, +)$ a cyclic group? If so, find the generators.

Yes, it is a cyclic group. There are two generators, $\langle 1 \rangle$ and $\langle -1 \rangle$

Problem 9. Let $\langle \zeta_n \rangle$ denote the set of the $n\text{-}th$ roots of unity. Show that $(\langle \zeta_n \rangle, *)$ is a group.

1. Associativity is true over the complex numbers.
2. We know that 1 is always a root of unity, $1 = e^{\frac{0*\pi}{n}}$
3. If $e^{\frac{2k\pi}{n}}$ is a root of unity, then $k \in \{0, 1, ..., n-1\}$. Therefore, $e^{\frac{2(n-k)\pi}{n}}$ is also a root of unity and is a multiplicative inverse

Problem 10. Consider S_3, the set of permutations of the set $\{1, 2, 3\}$. (Remember, these are the bijections $f : \{1, 2, 3\} \to \{1, 2, 3\}$.) Show that $(S_3, \circ)$ is non-abelian. In other words, find some $f, g \in S_3$ and $x \in \{1, 2, 3\}$ where $(g \circ f)(x) \neq (f \circ g)(x)$ (Remember, $\circ$ denotes composition. $(g \circ f)(x) = g(f(x))$).

Let $f(1) = 2$, $f(2) = 3$, $f(3) = 2$, $g(1) = 1$, $g(2) = 3$, $g(3) = 2$. Then $g(f(1)) = g(2) = 3$ but $f(g(1)) = f(1) = 2$, so $f(g(1)) \neq g(f(1))$.

As a thought exercise, you can consider the set $\{1, 2, 3\}$ as vertices of an equilateral triangle, where each permutation in S_3 moves around the vertices in a certain way with either a rotation or a reflection along certain axes.