Grade 9/10 Math Circles

March 29, 2023
An Introduction to Group Theory Part 2

Review from last time

Today we are going to learn about *symmetric groups*, and the relationship between symmetry groups and symmetric groups! But before we jump in, let's do a quick recap of last weeks lesson. Recall that a **group** is a set G, together with a binary operation $\bullet$, such that the following group axioms hold:

1. (Associativity) For every $a, b, c \in G$, $(a \bullet b) \bullet c = a \bullet (b \bullet c)$.

2. (Identity element) There exists $\text{id}_G \in G$ such that for all $a \in G$, $\text{id}_G \bullet a = a = a \bullet \text{id}_G$.

3. (Inverse element) For every $a \in G$, there exists $a^{-1} \in G$ such that $a \bullet a^{-1} = \text{id}_G = a^{-1} \bullet a$.
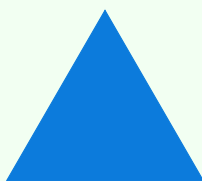
We write $(G, \bullet)$ to represent the group G with binary operation $\bullet$.

As an example, we saw that the integers

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

with addition form a group. In other words, $(\mathbb{Z}, +)$ is a group.

We also saw that the set of symmetries $\text{Sym}(S)$ of a shape S, such as the equilateral triangle below, with composition form a group. We will return to symmetry groups later in this lesson.

Symmetric Groups

Today we are going to focus on a special class of groups called *symmetric groups*. Like most classes of groups, symmetric groups appear all over mathematics. They are in particular important to the area of combinatorics! At the end of the lesson, we will see how the theory of symmetric groups can be used to solve a problem that has to do with "switching minds"! Recall again that a group is a set together with a binary operation. To get started, we first learn about this underlying set.

The underlying set of a symmetric group

The underlying set of a symmetric group is a certain collection of objects called *permutations*. You likely come across permutations in your every day life! For example, consider a full deck of cards:
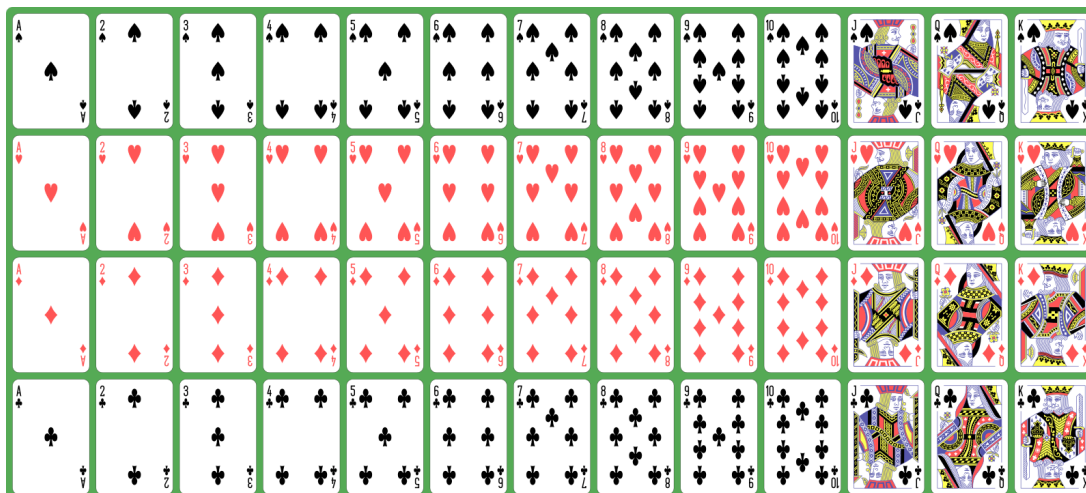

Figure 1: Standard deck of 52 cards[1]

A standard deck of cards contains 52 distinct cards. We consider cards with the same number to be distinct because they have different suits. Similarly, cards with the same suit are considered distinct because they have different numbers. Any shuffling of this deck of cards is an example of a *permutation*. So, in this example, we are looking at *permutations of cards*. In card games, the ordering of the cards in the deck matters and can affect the outcome of the game!

---

[1]Wikimedia Commons. English pattern playing cards deck [Online]. Available from: https://commons.wikimedia.org/wiki [Accessed March 24 2023].

There are two key things to note in this example:

1. Cards are being shuffled in various arrangements, and

2. The order of cards matters.

Together, these two key points describe what a permutation is!

Definition 1

If X is a set with a finite number of elements, meaning that X has n elements for some $n \in \mathbb{N}$, then we call X a **finite set**.

Note

The definition of set requires that all elements of a set are distinct. In other words, we don't allow duplicate objects to appear in a set. So, if X has n elements, this means that there are n **distinct** elements in X.

If X is a finite set, then roughly put, a *permutation* of X is an arrangement of its elements into some order.

Definition 2

Let X be a finite set. A **permutation** of X is an arrangement of the elements of X into some order such that every element of X appears in the arrangement exactly once.

The verb we use to describe the action of arranging the elements is **permute**. In present tense, we say that "we are **permuting** the elements of X".

Example 1

Let $X = \{a, b, c\}$. This is a finite set since there are 3 elements in it. Below are all possible permutations of X:

$$(a, b, c) \quad (a, c, b) \quad (b, a, c) \quad (b, c, a) \quad (c, a, b) \quad (c, b, a).$$

Note that the definition of permutation requires that every element of X appears **exactly once**. We

see that the arrangements in Example 1 satisfy this. Now, for instance, (a, b) is not a permutation of $X = \{a, b, c\}$ since c does not appear. Also, (a, b, b, c) is not a permutation of $X = \{a, b, c\}$ since b appears more than once.

Example 2

For another example, consider $X = \{1, 2, 3\}$. Below are all possible permutations of X:

$$(1, 2, 3) \quad (1, 3, 2) \quad (2, 1, 3) \quad (2, 3, 1) \quad (3, 1, 2) \quad (3, 2, 1).$$

Exercise 1

Let $X = \{1, 2, 3, 4\}$. List all of the permutations of X.

Stop and Think

Do you see a connection between the permutations in Example 1 and Example 2?

You may have noticed that the permutations in Example 1 and Example 2 are basically the same. More precisely, if we label a with the number 1, b with the number 2, and c with the number 3, then the permutations of $\{a, b, c\}$ are exactly the same as the permutations of $\{1, 2, 3\}$. In fact, this phenomenon is true in general! The permutations of a given set do not depend on what the *elements look like*, it only matters *how many elements* are in the set.

Let X be a finite set with $n \in \mathbb{N}$ elements. Going forward, we may assume that $n \geq 1$ because if $n = 0$, then X is the set containing no elements (i.e., the empty set) and so there are no elements to permute. Recall that the elements of a set are always distinct, meaning that there are no repeating elements. Since X has n distinct elements, we can write

$$X = \{x_1, \ldots, x_n\},$$

where $x_1, x_2, \ldots, x_n$ are considered to be all distinct from each other. In other words, we label each element of X with the symbol x_i for some $1 \leq i \leq n$. For example, we can label the elements of $\{a, b, c\}$ as $x_1 = a$, $x_2 = b$, and $x_3 = c$.

Notice that the permutations of X are the same as the permutations of $\{1, \ldots, n\}$. Why? Well, if we permute the elements x_i of X around, it's the same as permuting the indices i of the x_i around.

So, really, we are just permuting elements of the set $\{1, \ldots, n\}$. Because of this, we can assume that our sets take the form $\{1, \ldots, n\}$ for some $n \in \mathbb{N}$. This phenomenon tells us that finite sets with the same number of elements have the same permutations. So, we can make the following definition.

> **Definition 3**
>
> Let X be a finite set with n elements. The **set of permutations of X** is denoted by S_n.

Given a finite set X with $n \in \mathbb{N}$ elements, we can form the set S_n. The set S_n together with a certain binary operation forms a group. This group is called the **symmetric group** on X, or the **symmetric group** on $\{1, \ldots, n\}$. Let's learn about this binary operation on S_n.

Binary operation for symmetric groups

For each $n \in \mathbb{N}$, consider the set S_n. We want to find a binary operation on S_n. In other words, we want to find a way to combine two permutations of $\{1, \ldots, n\}$ into another permutation of $\{1, \ldots, n\}$. To do this, we introduce some new notation called **two-line notation**. It's a bit tricky to define this new notation without introducing more symbols, so we are going to explain the new notation using examples.

Example 3

Let $X = \{1, 2, 3\}$ and consider the permutation $\sigma = (2, 3, 1)$. The permutation σ shuffles the natural ordering $1, 2, 3$ into $2, 3, 1$. We can think of this as 1 being replaced by 2, 2 being replaced by 3, and 3 being replaced by 1. We can illustrate this information using the following diagram:

$$
\begin{array}{ccc}
1 & 2 & 3 \\
\downarrow & \downarrow & \downarrow \\
2 & 3 & 1
\end{array}
$$

In fact, we can think of σ as an operation that takes in 1 and outputs 2, takes in 2 and outputs 3, and takes in 3 and outputs 1. In words, it is common to say "1 goes to 2, 2 goes to 3, and 3 goes to 1". By ignoring the arrows in the above diagram, we can represent σ using the following **two-line notation**:

$$
\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.
$$

The top row is the inputs, the elements of the set X. The bottom row is the outputs, the values each number is mapped to.

Example 4

Let $X = \{1, 2, 3, 4\}$ and consider the permutation $\sigma = (1, 3, 4, 2)$. In our new notation, we write

$$
\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}.
$$

Given permutations $\sigma, \beta \in S_n$, we can combine them to make a new permutation $\sigma \circ \beta$ in S_n. The permutation $\sigma \circ \beta$ is read as the **composition** of σ with β. In general, note that the permutation $\sigma \circ \beta$ is not necessarily equal to the permutation $\beta \circ \sigma$.

Composition is a binary operation on S_n.

Defining the binary operation **composition** on S_n requires a lot of extra notation, so we will learn how it works through examples.

Example 5

Let $X = \{1, 2, 3\}$ and consider the following two permutations in S_3

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

The composition $\sigma \circ \beta$ is given as follows:

$$\sigma \circ \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Let's explain how we got this. Looking at β, we see that 1 goes to 1. We then look at σ to see where 1 goes. In σ see that 1 goes to 2. So the result is that 1 goes to 2. This is where the first column of $\sigma \circ \beta$ comes from. Next, looking at β we see that 2 goes to 3. Then looking at σ we see that 3 goes to 1. So the result is that 2 goes to 1. This is where the second column of $\sigma \circ \beta$ comes from. Lastly, looking at β we see that 3 goes to 2. Then looking at σ we see that 2 goes to 3. So the result is that 3 goes to 3. This is where the third column of $\sigma \circ \beta$ comes from. We can think of $\sigma \circ \beta$ as first shuffling $1, 2, 3$ into $1, 3, 2$ and then shuffling $1, 3, 2$ according to σ.

Example 6

Let $X = \{1, 2, 3, 4\}$ and consider the following two permutations of S_4

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

Then

$$\sigma \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} \quad \text{and} \quad \beta \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}.$$

This example illustrates that $\sigma \circ \beta \neq \beta \circ \sigma$. Here, the symbol $\neq$ means "not equal".

Exercise 2

Let $X = \{1, 2, 3, 4, 5\}$ and consider the following two permutations of S_5

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix} \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{pmatrix}.$$

Compute the compositions $\sigma \circ \beta$ and $\beta \circ \sigma$.

Exercise 3

Convince yourself that $(S_3, \circ)$ is a group.

** See solutions to Exercise 3 before reading on **

The explanation in Exercise 3 can be generalized to show that $(S_n, \circ)$ is a group for any $n \in \mathbb{N}$. So, in general, S_n with composition forms a group! Let's sketch how this works. To do this, we need to convince ourselves that the group axioms hold for S_n with composition $\circ$. So, let $\sigma, \beta, \alpha \in S_n$.

Axiom 1: For associativity to hold, we need $(\sigma \circ \beta) \circ \alpha$ to be the same permutation as $\sigma \circ (\beta \circ \alpha)$. Similar to symmetry groups, this axiom is a bit tough to argue given our current mathematical tools. As mentioned in Example 5, we can view permutations as operations, or more formally as functions. If you know a bit about functions, then by viewing each permutations as a function, it isn't too hard to show that

$$(\sigma \circ \beta) \circ \alpha = \sigma \circ \beta \circ \alpha = \sigma \circ (\beta \circ \alpha).$$

If you were able to convince yourself that associativity holds in Exercise 3, that is plenty good enough!

Axiom 2: Not shuffling $1, 2, \ldots, n$ out of it's natural ordering is a valid permutation of $\{1, \ldots, n\}$. In other words,

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$$

is a permutation in S_n. This is the identity element in S_n because if you compose this permutation with σ you get σ back. We write

$$\mathrm{id}_{S_n} = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

Axiom 3: Lastly, given a permutation σ in S_n we can construct it's inverse σ^{-1} as follows. Write

σ using the two-line notation. The inverse σ^{-1} of σ is obtained by switching the rows of σ and then reordering the columns so that the top row is in the order $1, \ldots, n$.


Definition 4

We call the group $(S_n, \circ)$ the **symmetric group** on $\{1, \ldots, n\}$.

## Relationship between symmetry groups and symmetric groups

We are going to first compare the symmetry group of the equilateral triangle with the symmetric group on $\{1, 2, 3\}$. Last time we saw that the symmetries of the equilateral triangle are

- counter-clockwise rotations by multiples of 120 degrees, and

- reflections in the 3 axes that pass through the center and a tip of the triangle.

If we label the tips of the triangle with the numbers 1,2,3 then we can view the symmetries of the triangle as certain permutations of $\{1, 2, 3\}$. It doesn't matter how we label the triangle, but we will use the labelling below for this lesson:
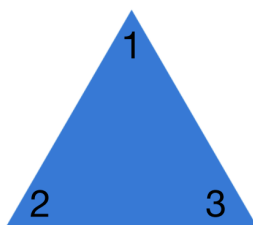

Just as a permutation in S_3 shuffles the natural ordering $1, 2, 3$, a symmetry of the triangle shuffles the positions of the numbers on the triangle above. Let's see how symmetries of the triangle can be identified with permutations in S_3. First consider the symmetry which is counter-clockwise rotation by 120 degrees:
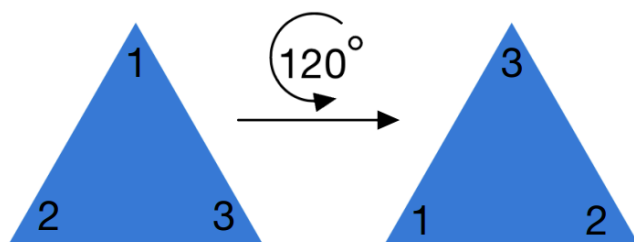
We see that this symmetry moves 1 from the top tip of the triangle to the left tip, 2 from the left tip to the right tip, and 3 from the right tip to the top tip. Alternatively, we can think of this as 1 moving to where 2 was, 2 moving to where 3 was, and 3 moving to where 1 was. In words, we can say "1 goes to 2, 2 goes to 3, and 3 goes to 1" (sound familiar? See Example 3). Given this, this symmetry corresponds to the permutation

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Next, consider counter-clockwise rotation by 240 degrees:
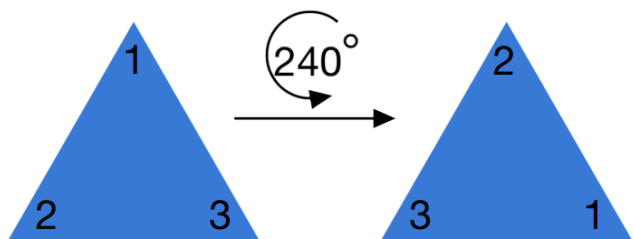
Similar to above, this symmetry sends 1 to 3, 2 to 1, and 3 to 2. In words, we can say 1 goes to 3, 2 goes to 1, and 3 goes 2. Given this, this symmetry corresponds to the the permutation
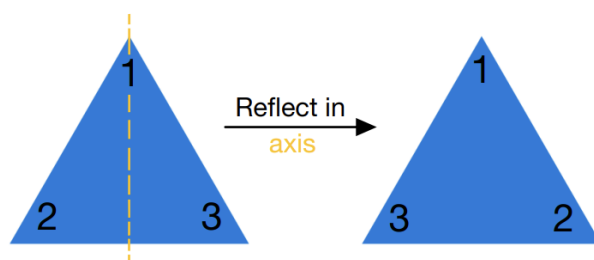
$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

The last rotation symmetry of the triangle is counter-clockwise rotation by 360 degrees, or equivalently, the identity symmetry which "does nothing":
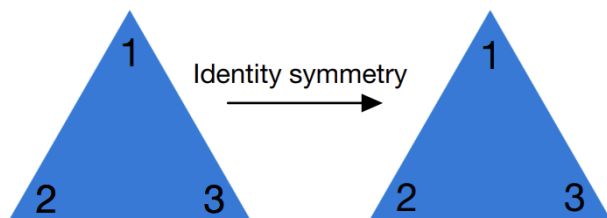
This symmetry does nothing, and so the positions of the numbers on the triangle do not change. Here, we say 1 goes to 1, 2 goes to 2, and 3 goes to 3. To no surprise, the identity symmetry of the triangle corresponds to the identity permutation

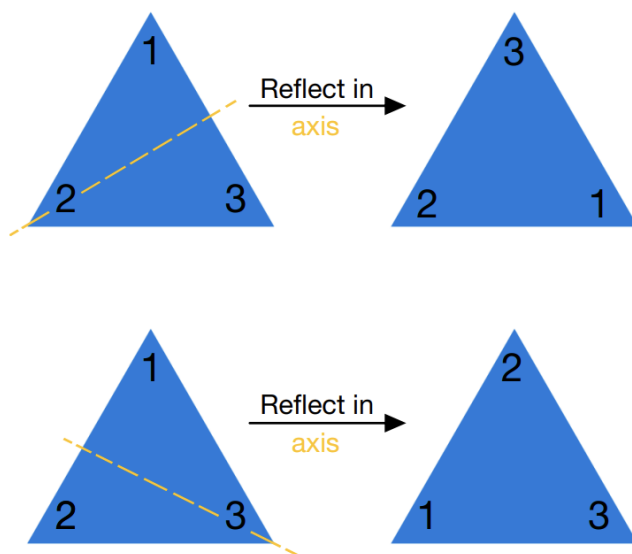$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}.$$

Next, consider the symmetry that reflects in the yellow axis drawn below:

This symmetry fixes 1 in the top position, but interchanges 2 and 3. So, we can say 1 goes to 1, 2 goes to 3, and 3 goes to 2. This symmetry corresponds to the permutation

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

The permutations corresponding to the last two symmetries

are

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

respectively. The above shows us that every permutation in S_3 corresponds to a unique symmetry of the triangle. Note that if you compose two symmetries of the triangle, it's the same as composing the two permutations that correspond to the symmetries. For example, the composition of "counter-clockwise rotation by 120 degrees" with "counter-clockwise rotation by 240 degrees" rotates the triangle a full 360 degrees, and so the composition is the identity symmetry. So, we should expect that the composition of the corresponding permutations is the identity permutation. Indeed, we have that

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \text{id}_{S_3}.$$

Given these correspondences, or identifications, there is no harm in saying that the symmetry group of the triangle is the *same* as the symmetric group on $\{1, 2, 3\}$.

We can play the same game as above by identifying symmetries of a regular polygon that has n sides with permutations of $\{1, \ldots, n\}$. However, in general it is not true that the symmetry group of a regular polygon with n sides is the same as the symmetric group on $\{1, \ldots, n\}$.

Exercise 4

Show that the symmetry group of the square (i.e., regular polygon with 4 sides) is **not** the same as the symmetric group on $\{1, 2, 3, 4\}$. To get started, consider the following labelling of the square:
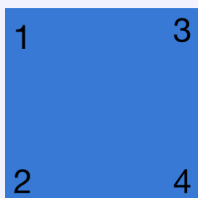
Application to symmetric groups: The Futurama Theorem

We are going to end this lesson with an application to symmetric groups! The problem we are going to discuss today was developed and proved in the episode "The Prisoner of Benda" for the TV show Futurama. In fact, the mathematician Ken Keeler, who wrote this episode, came up with this theorem and proved it specifically for the show. The statement of the problem is known as *The Futurama Theorem*. Let's discuss the problem introduced in this episode.

In the episode, two characters of the show, Amy and Professor Farnsworth, build a machine that allows them to switch minds! They decide to test the machine out, and switch minds. They are initially very excited, but then quickly realize that they aren't able to switch their minds back. After reviewing their calculations, they realize that they failed to take into account the "cerebral immune response" of the brain, and as a result, once two bodies switch minds they can never directly switch back using the machine. In other words, the mind swap machine can't be used on the same pair of beings more than once.

Figure 2: Amy (left) and Professor Farnsworth (right) using their mind switching machine.[2]

To summarize so far:

- We have a mind switching machine!

- If two beings sit in the chairs, they can switch minds.

- **Rule**: Any two beings can use the machine at most once to switch minds.

Amy and Professor Farnsworth are panicking a bit now. They want to switch their minds back, but the machine won't allow them! They come up with the idea of swapping minds back by using a third body for temporary storage space. For a third body, the robot Bender comes to help. Before we switch more minds, let's introduce pictures that will help us keep track of which mind is in which body.
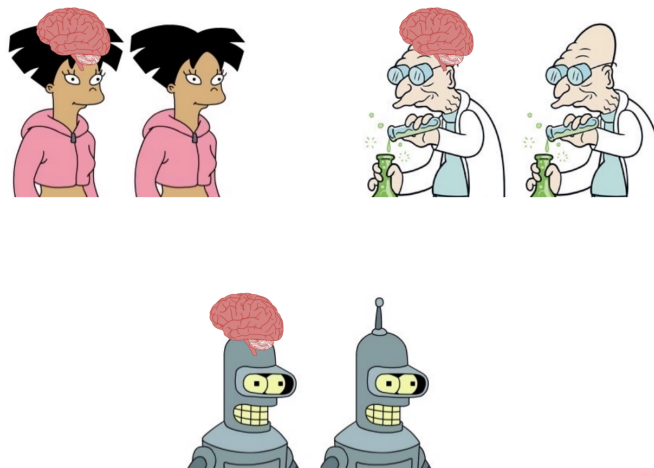

Figure 3: The 3 characters. Bender is at the bottom.[3]

We use 2 photos for each character. The photo with the brain is used to represent the mind of that character. The photo without the brain is used to represent the body of that character. We can represent the first mind switch using the following photos:
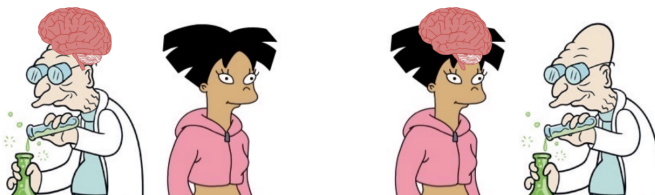

Figure 4: Amy and Professor Farnsworth switch minds.

The 2 photos on the left indicate that Professor Farnsworth's mind is in Amy's body. The 2 photos on the right indicate that Amy's mind is in Professor Farnsworth's body. Now, they introduce Bender as a way to try and get their minds back. In the show, the robot Bender sits down in the mind machine with Amy' body (Farnsworth's mind). They switch minds so that Bender's mind is now in Amy's body and Farnsworth's mind is now in Bender's body. So far, we have:
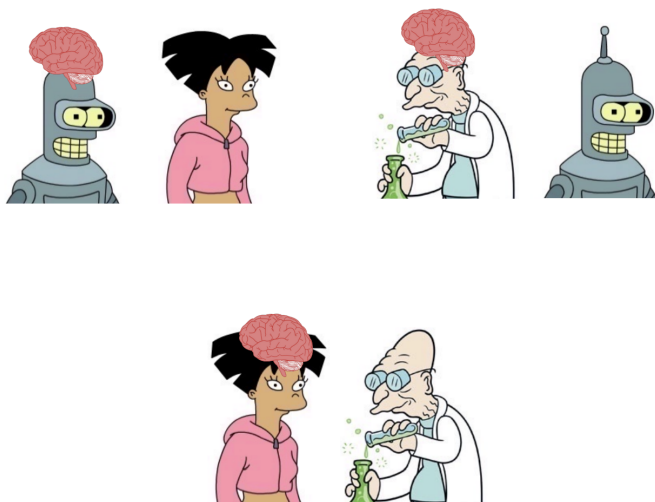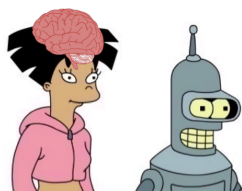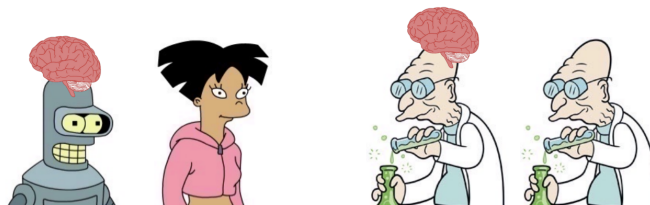

Amy's body and Farnsworth's body already switched minds, so they can't switch again. Similarly,

---

[2]Mathologer. The Futurama Theorem [Online]. Available from: https://www.youtube.com/watch?v=J65GNFfL94c [Accessed March 24 2023].

[3]All character photos in this lesson are from: Futurama Fandom. Futurama wiki characters [Online]. Available from: https://futurama.fandom.com/wiki/Characters [Accessed March 24 2023].

Amy's body and Bender's body already switched minds, so they can't switch again. Given this, the only swap that can be made is between Bender's body and Farnsworth's body. This results in:

This was somewhat successful in the sense that Farnsworth's mind is back in their body. However, since Amy's body and Bender's body already swapped minds they can't switch back! We are essentially back to the same problem as before. In the episode, they try to fix the problem by bringing even more bodies into play. After doing many mind switches, they end up with a big mess!

Exercise 5

Consider the original situation where only Amy and Professor Farnsworth have switched minds (see Figure 3).

1. Can we get Amy's mind back into Amy's body and Farnsworth's mind back into Farnsworth's body?

2. Further, can (1) be done in such a way that everyone who switches minds ends up with their own mind in the end?

∗∗ See solutions to Exercise 5 before reading on ∗∗

As you have seen, the answer to both questions in Exercise 5 is yes. And this is true in general. That is, if we switch as many minds as we want, then it's true that we can always reverse the minds swaps so that everyone gets their own mind back. This leads us to the theorem mentioned at the beginning of this section.

> **Futurama Theorem**
>
> Given a mind swap machine that can't be used on the same pair of beings more than once, it is possible to reverse any number of mind swaps by introducing two more beings that did not have their minds swapped with anyone before.
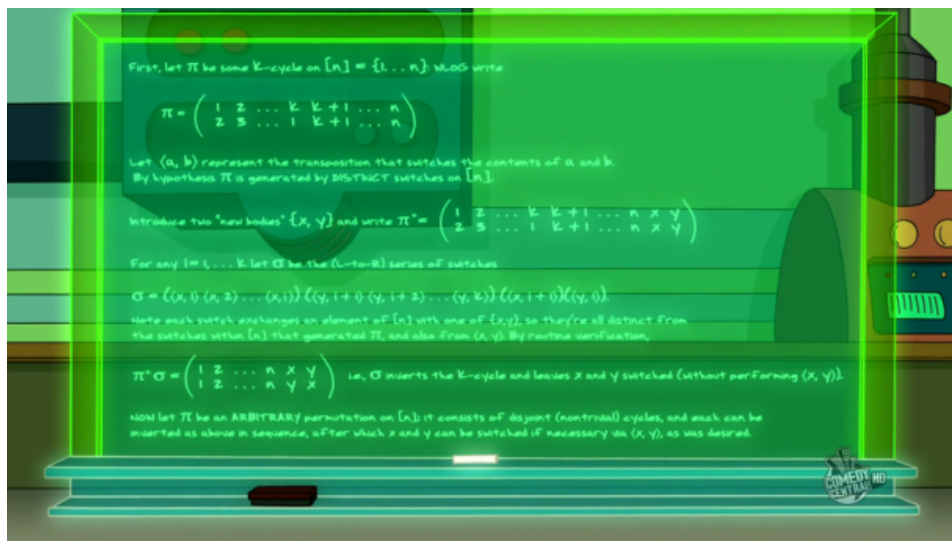

Figure 5: Ken Keeler's proof of the Futurama Theorem appearing in the episode[2]

To understand Ken's proof of the Futurama Theorem, as displayed in Figure 4, it is enough to go through the proof for the case when only 2 beings switch minds. You technically have done this already! The solution to Exercise 5 is the proof of this case. Ken's proof is just in the language of groups theory. We won't go through the details of how to translate the solution to Exercise 5 into group theory, but the basic idea is as follows. By putting the characters bodies in a fixed order, you can interpret mind swaping as permuting the brains of the characters around. That is, mind swaps are permutations of brains!