What is a group and why should I care?

Daniel Platt

October 10, 2019

◆□▶ ◆□▶ ◆ □▶ ◆ □▶ ● □ ● ● ● ●

Very general mathematical concept, can be applied to:



◆□▶ ◆□▶ ◆ □▶ ◆ □▶ ● □ ● ● ● ●



Symmetry Group of the Cube

Very general mathematical concept, can be applied to:



The Real Numbers



Real life applications:

https://www...

"Elliptic Curves Cryptography": send messages across the internet that can only be read by the recipient

◆□▶ ◆□▶ ◆□▶ ▲□▶ ▲□ ◆ ○ ◆ ○ ◆

Real life applications:



Infrared Spectroscopy: Find out what molecules are contained in a sample without having to touch it

Real life applications:



DNA and braid groups: DNA is a long thing, tangled up; biologists want to understand how exactly it is tangled

・ロト ・ 四 ト ・ ヨ ト ・ ヨ ト ・ ヨ

Definition

A *group* is a set of elements together with an operation that combines any two elements to form a third element, satisfying some properties.

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

Definition

A *group* is a set of elements together with an operation that combines any two elements to form a third element, satisfying some properties.

Example

Set = $\{ \diamondsuit, \diamondsuit, \heartsuit \}$, operation \circ given by

0	•	•	\heartsuit
¢	¢	÷	\heartsuit
*	÷	\heartsuit	¢
\heartsuit	\heartsuit	¢	÷

◆□▶ ◆□▶ ◆□▶ ▲□▶ ▲□ ◆ ○ ◆ ○ ◆

Definition

A *group* is a set of elements together with an operation that combines any two elements to form a third element, satisfying some properties.

Example

Set = { \diamondsuit , \diamondsuit , \heartsuit }, operation \circ given by



E.g.
$$\blacklozenge \circ \heartsuit = \heartsuit$$

Definition

A *group* is a set of elements together with an operation that combines any two elements to form a third element, satisfying some properties.

Example

Set = { \diamondsuit , \diamondsuit , \heartsuit }, operation \circ given by



E.g.
$$\blacklozenge \circ \heartsuit = \heartsuit$$
, $\blacklozenge \circ (\clubsuit \circ \clubsuit) =$

Definition

A *group* is a set of elements together with an operation that combines any two elements to form a third element, satisfying some properties.

Example

Set = { \diamondsuit , \diamondsuit , \heartsuit }, operation \circ given by



E.g.
$$\boldsymbol{\uparrow} \circ \heartsuit = \heartsuit, \ \boldsymbol{\uparrow} \circ (\boldsymbol{\clubsuit} \circ \boldsymbol{\clubsuit}) = \heartsuit$$
.

Definition

A *group* is a set of elements together with an operation that combines any two elements to form a third element, satisfying the following properties:

▲□▶ ▲□▶ ▲ □▶ ▲ □▶ □ のへぐ

Definition

A *group* is a set of elements together with an operation that combines any two elements to form a third element, satisfying the following properties:

◆□▶ ◆□▶ ◆□▶ ▲□▶ ▲□ ◆ ○ ◆ ○ ◆

(x, y, z are any group elements, and \circ denotes the group operation)

Definition

A *group* is a set of elements together with an operation that combines any two elements to form a third element, satisfying the following properties:

◆□▶ ◆□▶ ◆□▶ ▲□▶ ▲□ ◆ ○ ◆ ○ ◆

(x, y, z are any group elements, and \circ denotes the group operation)

1. Neutral Element: There exists an element e, such that

 $e \circ x = x$ and $x \circ e = x$;

Definition

A *group* is a set of elements together with an operation that combines any two elements to form a third element, satisfying the following properties:

(x, y, z are any group elements, and \circ denotes the group operation)

- 1. *Neutral Element*: There exists an element e, such that $e \circ x = x$ and $x \circ e = x$;
- 2. *Inverse Element*: For every x there exists some y, such that $x \circ y = e$ and $y \circ x = e$.

◆□▶ ◆□▶ ◆□▶ ▲□▶ ▲□ ◆ ○ ◆ ○ ◆

Definition

A *group* is a set of elements together with an operation that combines any two elements to form a third element, satisfying the following properties:

(x, y, z are any group elements, and \circ denotes the group operation)

- 1. *Neutral Element*: There exists an element e, such that $e \circ x = x$ and $x \circ e = x$;
- 2. *Inverse Element*: For every x there exists some y, such that $x \circ y = e$ and $y \circ x = e$.

◆□▶ ◆□▶ ◆□▶ ▲□▶ ▲□ ◆ ○ ◆ ○ ◆



Definition

A *group* is a set of elements together with an operation that combines any two elements to form a third element, satisfying the following properties:

(x, y, z are any group elements, and \circ denotes the group operation)

- 1. *Neutral Element*: There exists an element e, such that $e \circ x = x$ and $x \circ e = x$;
- 2. *Inverse Element*: For every x there exists some y, such that $x \circ y = e$ and $y \circ x = e$.



Neutral element: Inverse element for \clubsuit : Inverse element for \clubsuit : Inverse element for \heartsuit :

Definition

A *group* is a set of elements together with an operation that combines any two elements to form a third element, satisfying the following properties:

(x, y, z are any group elements, and \circ denotes the group operation)

- 1. *Neutral Element*: There exists an element e, such that $e \circ x = x$ and $x \circ e = x$;
- 2. *Inverse Element*: For every x there exists some y, such that $x \circ y = e$ and $y \circ x = e$.



Neutral element: \blacklozenge Inverse element for \clubsuit : Inverse element for \clubsuit : Inverse element for \heartsuit :

Definition

A *group* is a set of elements together with an operation that combines any two elements to form a third element, satisfying the following properties:

(x, y, z are any group elements, and \circ denotes the group operation)

- 1. *Neutral Element*: There exists an element e, such that $e \circ x = x$ and $x \circ e = x$;
- 2. *Inverse Element*: For every x there exists some y, such that $x \circ y = e$ and $y \circ x = e$.



Neutral element: \blacklozenge Inverse element for \clubsuit : \blacklozenge Inverse element for \clubsuit : Inverse element for \heartsuit :

Definition

A *group* is a set of elements together with an operation that combines any two elements to form a third element, satisfying the following properties:

(x, y, z are any group elements, and \circ denotes the group operation)

- 1. *Neutral Element*: There exists an element e, such that $e \circ x = x$ and $x \circ e = x$;
- 2. *Inverse Element*: For every x there exists some y, such that $x \circ y = e$ and $y \circ x = e$.



Neutral element: \blacklozenge Inverse element for \clubsuit : \diamondsuit Inverse element for \clubsuit : \heartsuit Inverse element for \heartsuit :

Definition

A *group* is a set of elements together with an operation that combines any two elements to form a third element, satisfying the following properties:

(x, y, z are any group elements, and \circ denotes the group operation)

- 1. *Neutral Element*: There exists an element e, such that $e \circ x = x$ and $x \circ e = x$;
- 2. *Inverse Element*: For every x there exists some y, such that $x \circ y = e$ and $y \circ x = e$.



Neutral element: \blacklozenge Inverse element for \clubsuit : \diamondsuit Inverse element for \clubsuit : \heartsuit Inverse element for \heartsuit : \clubsuit

Task: Hang a picture on two nails, so that it falls down if *either* nail is pulled out.



Idea: Write path of the rope as formula If rope passes left nail write *a* if it crosses the dotted line clockwise and a^{-1} for counter-clockwise Analog for right nail with letters *b* and b^{-1}



Idea: Write path of the rope as formula If rope passes left nail write *a* if it crosses the dotted line clockwise and a^{-1} for counter-clockwise Analog for right nail with letters *b* and b^{-1}



(日)

Idea: Write path of the rope as formula If rope passes left nail write *a* if it crosses the dotted line clockwise and a^{-1} for counter-clockwise Analog for right nail with letters *b* and b^{-1}



(日)

Idea: Write path of the rope as formula If rope passes left nail write *a* if it crosses the dotted line clockwise and a^{-1} for counter-clockwise Analog for right nail with letters *b* and b^{-1}



イロト イポト イヨト

3

Idea: Write path of the rope as formula If rope passes left nail write *a* if it crosses the dotted line clockwise and a^{-1} for counter-clockwise Analog for right nail with letters *b* and b^{-1}



(日)

for rope formulae: write next to each other

for rope formulae: write next to each other $(ab) \circ (a^{-1}) =$

for rope formulae: write next to each other $(ab) \circ (a^{-1}) = aba^{-1}$



▲ロ ▶ ▲周 ▶ ▲ 国 ▶ ▲ 国 ▶ ● ● ● ● ● ●

for rope formulae: write next to each other $(ab) \circ (a^{-1}) = aba^{-1}$



▲ロ ▶ ▲周 ▶ ▲ 国 ▶ ▲ 国 ▶ ● ● ● ● ● ●

1. What is the neutral element here?

for rope formulae: write next to each other $(ab) \circ (a^{-1}) = aba^{-1}$



- 1. What is the neutral element here?
- 2. What are the inverse elements? For example: Inverse of ab is

▲ロ ▶ ▲周 ▶ ▲ 国 ▶ ▲ 国 ▶ ● ● ● ● ● ●

$$b^{-1}a^{-1}$$
 because
 $abb^{-1}a^{-1} = aa^{-1}$
Inverse of aab^{-1} ?

for rope formulae: write next to each other $(ab) \circ (a^{-1}) = aba^{-1}$



- 1. What is the neutral element here?
- 2. What are the inverse elements? For example: Inverse of *ab* is $b^{-1}a^{-1}$ because

・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・

 $abb^{-1}a^{-1} = aa^{-1}$ Inverse of aab^{-1} ?

3. What happens to a formula when a nail is pulled out?

for rope formulae: write next to each other $(ab) \circ (a^{-1}) = aba^{-1}$



- 1. What is the neutral element here?
- 2. What are the inverse elements? For example: Inverse of *ab* is $b^{-1}a^{-1}$ because $abb^{-1}a^{-1} = aa^{-1}$

Inverse of aab^{-1} ?

3. What happens to a formula when a nail is pulled out?

Solution for the puzzle? How about 3 nails?

for rope formulae: write next to each other $(ab) \circ (a^{-1}) = aba^{-1}$



- 1. What is the neutral element here?
- 2. What are the inverse elements? For example: Inverse of *ab* is $b^{-1}a^{-1}$ because $abb^{-1}a^{-1} = aa^{-1}$

Inverse of aab^{-1} ?

3. What happens to a formula when a nail is pulled out?

Solution for the puzzle? How about 3 nails? Test in real life!



for rope formulae: write next to each other $(ab) \circ (a^{-1}) = aba^{-1}$



- 1. What is the neutral element here?

Inverse of aab^{-1} ?

3. What happens to a formula when a nail is pulled out?

Solution for the puzzle? How about 3 nails? Test in real life!



0

for rope formulae: write next to each other $(ab) \circ (a^{-1}) = aba^{-1}$



- 1. What is the neutral element here?
- 2. What are the inverse elements? For example: Inverse of *ab* is $b^{-1}a^{-1}$ because $abb^{-1}a^{-1} = aa^{-1}$ Inverse of aab^{-1} ?

 $ba^{-1}a^{-1}$

0

3. What happens to a formula when a nail is pulled out?

Solution for the puzzle? How about 3 nails? Test in real life!



for rope formulae: write next to each other $(ab) \circ (a^{-1}) = aba^{-1}$



- 1. What is the neutral element here?
- 2. What are the inverse elements? For example: Inverse of *ab* is $b^{-1}a^{-1}$ because $abb^{-1}a^{-1} = aa^{-1}$

Inverse of aab^{-1} ?

 $ba^{-1}a^{-1}$

0

3. What happens to a formula when a nail is pulled out? $aba^{-1} \xrightarrow{\text{pull b}} aba^{-1} = aa^{-1} = 0$

Solution for the puzzle? How about 3 nails? Test in real life!



For two nails:

For two nails:

$$aba^{-1}b^{-1}$$

pull out left nail $\rightarrow aba^{-1}b^{-1} = bb^{-1} = 0$
pull out right nail $\rightarrow aba^{-1}b^{-1} = aa^{-1} = 0$

For two nails:

$$aba^{-1}b^{-1}$$

pull out left nail $\rightarrow aba^{-1}b^{-1} = bb^{-1} = 0$
pull out right nail $\rightarrow aba^{-1}b^{-1} = aa^{-1} = 0$

◆□▶ ◆□▶ ◆ □▶ ◆ □▶ ● □ ● ● ● ●

For three nails: write $x = aba^{-1}b^{-1}$

For two nails:

$$aba^{-1}b^{-1}$$

pull out left nail $\rightarrow aba^{-1}b^{-1} = bb^{-1} = 0$
pull out right nail $\rightarrow aba^{-1}b^{-1} = aa^{-1} = 0$

For three nails: write $x = aba^{-1}b^{-1}$

1. What is x^{-1} ? (I.e. x "grouped with" what gives 0?)

For two nails:

$$aba^{-1}b^{-1}$$

pull out left nail $\rightarrow aba^{-1}b^{-1} = bb^{-1} = 0$
pull out right nail $\rightarrow aba^{-1}b^{-1} = aa^{-1} = 0$

◆□▶ ◆□▶ ◆ □▶ ◆ □▶ ● □ ● ● ● ●

For three nails: write $x = aba^{-1}b^{-1}$

1. What is
$$x^{-1}$$
? (I.e. x "grouped with" what gives 0?)
 $x^{-1} = bab^{-1}a^{-1}$

For two nails:

$$aba^{-1}b^{-1}$$

pull out left nail $\rightarrow aba^{-1}b^{-1} = bb^{-1} = 0$
pull out right nail $\rightarrow aba^{-1}b^{-1} = aa^{-1} = 0$

For three nails: write $x = aba^{-1}b^{-1}$

- 1. What is x^{-1} ? (I.e. x "grouped with" what gives 0?) $x^{-1} = bab^{-1}a^{-1}$
- 2. How can you construct a solution from c, c^{-1} , x, x^{-1} ?

◆□▶ ◆□▶ ◆□▶ ▲□▶ ▲□ ◆ ○ ◆ ○ ◆

For two nails:

$$aba^{-1}b^{-1}$$

pull out left nail $\rightarrow aba^{-1}b^{-1} = bb^{-1} = 0$
pull out right nail $\rightarrow aba^{-1}b^{-1} = aa^{-1} = 0$

For three nails: write $x = aba^{-1}b^{-1}$

- 1. What is x^{-1} ? (I.e. x "grouped with" what gives 0?) $x^{-1} = bab^{-1}a^{-1}$
- 2. How can you construct a solution from c, c^{-1} , x, x^{-1} ?

$$xcx^{-1}c^{-1} = aba^{-1}b^{-1}cbab^{-1}a^{-1}c^{-1}$$

▲ロ ▶ ▲周 ▶ ▲ 国 ▶ ▲ 国 ▶ ● ● ● ● ● ●

3. What about *n* nails?

For two nails:

$$aba^{-1}b^{-1}$$

pull out left nail $\rightarrow aba^{-1}b^{-1} = bb^{-1} = 0$
pull out right nail $\rightarrow aba^{-1}b^{-1} = aa^{-1} = 0$

For three nails: write $x = aba^{-1}b^{-1}$

- 1. What is x^{-1} ? (I.e. x "grouped with" what gives 0?) $x^{-1} = bab^{-1}a^{-1}$
- 2. How can you construct a solution from c, c^{-1} , x, x^{-1} ?

$$xcx^{-1}c^{-1} = aba^{-1}b^{-1}cbab^{-1}a^{-1}c^{-1}$$

3. What about *n* nails? Let *y* be a solution for n - 1 nails, then $yny^{-1}n^{-1}$ is a solution for *n* nails

Braid Groups

2 sticks with 3 parallel strings

rotate bottom stick by 360°

Question: you are allowed to rotate the strings around the sticks. Can the strings be untangled? What about a 720° rotation?



Braid Groups

"rotating a string around a stick" means to take the string all the way around:



(In the above example: Don't stop after pulling the white string half way around the stick, i.e. after crossing the white and the red string. If that was allowed, the puzzle would be too easy). $(a \ge b \ge c)$

Braid Groups

Idea: Write braid as braid word

left strand over middle strand = s_1 , left under middle = s_1^{-1} middle strand over right strand = s_2 , middle under right = s_2^{-1}



for braid words:

for braid words: write words next to each others

for braid words: write words next to each others

$$(s_1s_1)\circ(s_2^{-1})=s_1s_1s_2^{-1}$$

◆□▶ ◆□▶ ◆ □▶ ◆ □▶ ● □ ● ● ● ●

for braid words: write words next to each others

$$(s_1s_1)\circ(s_2^{-1})=s_1s_1s_2^{-1}$$

for pictures: arrange under each other

for braid words: write words next to each others

$$(s_1s_1)\circ(s_2^{-1})=s_1s_1s_2^{-1}$$

▲□▶ ▲□▶ ▲□▶ ▲□▶ □ のQで

for pictures: arrange under each other



for braid words: write words next to each others

$$(s_1s_1)\circ(s_2^{-1})=s_1s_1s_2^{-1}$$

for pictures: arrange under each other



What are the braid words for these braids?











What are the braid words for these braids?











What are the braid words for these braids?











・ロト・日本・日本・日本・日本・日本

What are the braid words for these braids?









What are the braid words for these braids?











Solving the puzzle: How does the braid word change when

1. rearranging crossings?



2. moving one of the outermost strings around one stick?



Use 1. and 2. to go from the formula for the 360° braid or 720° braid to the trivial formula. Is it possible? Try something like: $s_1 \underline{s_2 s_1 s_2} s_1 s_2 = s_1 \underline{s_1 s_2 s_1 s_1} \underline{s_2} = s_1 \underline{s_1}$

ъ



Solving the puzzle: How does the braid word change when

1. rearranging crossings?







2. moving one of the outermost strings around one stick?



Use 1. and 2. to go from the formula for the 360° braid or 720° braid to the trivial formula. Is it possible? Try something like: $s_1 \underline{s_2 s_1 s_2} s_1 \underline{s_2} = s_1 \underline{s_1 s_2 s_1 s_2} = s_1 \underline{s_1}$

- 1. What are the braid words of the 360° and 720° braids?
- 2. How can we change the braid word with our allowed motions?
- 3. Can one apply the rules from 2. and 3. to go from the braid word of the 720° braids to the neutral element?

◆□▶ ◆□▶ ◆□▶ ▲□▶ ▲□ ◆ ○ ◆ ○ ◆

- 2. How can we change the braid word with our allowed motions?
- 3. Can one apply the rules from 2. and 3. to go from the braid word of the 720° braids to the neutral element?

◆□▶ ◆□▶ ◆□▶ ▲□▶ ▲□ ◆ ○ ◆ ○ ◆

4. What about the 360° braid?

- 2. How can we change the braid word with our allowed motions? $s_1s_2s_2s_1 = 0$, $s_2s_1s_1s_2 = 0$, $s_2s_2s_1s_1 = 0$, $s_1s_2s_1 = s_2s_1s_2$
- 3. Can one apply the rules from 2. and 3. to go from the braid word of the 720° braids to the neutral element?

・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・

- 2. How can we change the braid word with our allowed motions? $s_1s_2s_2s_1 = 0$, $s_2s_1s_1s_2 = 0$, $s_2s_2s_1s_1 = 0$, $s_1s_2s_1 = s_2s_1s_2$
- 3. Can one apply the rules from 2. and 3. to go from the braid word of the 720° braids to the neutral element?

・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・

- 2. How can we change the braid word with our allowed motions? $s_1s_2s_2s_1 = 0$, $s_2s_1s_1s_2 = 0$, $s_2s_2s_1s_1 = 0$, $s_1s_2s_1 = s_2s_1s_2$
- 3. Can one apply the rules from 2. and 3. to go from the braid word of the 720° braids to the neutral element?

$$(s_1s_2)^6 = s_1s_2s_1s_2s_1s_2s_1s_2s_1s_2s_1s_2s_1s_2$$

= $s_1s_2s_2s_1s_2s_2s_1s_1s_2s_1s_1s_2$
= $\underbrace{s_1s_2s_2s_1}\underbrace{s_2s_2s_1s_1}\underbrace{s_2s_1s_1s_2}\underbrace{s_2s_1s_1s_2}=0$

・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・

"Take every string around the stick exactly once!"

- 2. How can we change the braid word with our allowed motions? $s_1s_2s_2s_1 = 0$, $s_2s_1s_1s_2 = 0$, $s_2s_2s_1s_1 = 0$, $s_1s_2s_1 = s_2s_1s_2$
- 3. Can one apply the rules from 2. and 3. to go from the braid word of the 720° braids to the neutral element?

$$(s_1s_2)^6 = s_1s_2s_1s_2s_1s_2s_1s_2s_1s_2s_1s_2s_1s_2$$

= $s_1s_2s_2s_1s_2s_2s_1s_1s_2s_1s_1s_2$
= $\underbrace{s_1s_2s_2s_1}\underbrace{s_2s_2s_1s_1}\underbrace{s_2s_1s_1s_2}\underbrace{s_2s_1s_1s_2}=0$

4. What about the 360° braid? Impossible! $s_1s_2s_1s_2s_1s_2$ has 6 letters. Applying rules changes number by $4 \rightarrow$ can never reach 0

・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・