Group Theory

Sophia Hou and Jaeyi Song

MIT PRIMES Circle

May 21st, 2022

Introduction

Jaeyi

Jaeyi

Hello, my name is Jaeyi Song and I am a freshman.

Jaeyi

Hello, my name is Jaeyi Song and I am a freshman.

My interests include science research, music, and playing with my dog.

Jaeyi

Hello, my name is Jaeyi Song and I am a freshman.

My interests include science research, music, and playing with my dog.

Sophia

Sophia

Hi, my name is Sophia Hou and I'm a sophomore.

Sophia

Hi, my name is Sophia Hou and I'm a sophomore.

One fun fact is that I have a younger sister.

Groups

Introduction to Groups

Introduction to Groups

Definition

A **group** $(G, +)$ is a set G with a binary operation $*$ that has three requirements satisfied:

1. Associativity: $a * (b * c) = (a * b) * c$ for all elements $a, b, c \in G$.
2. Identity: there is an element $e \in G$ in which $a * e = e * a = a$ for all elements of G. The identity for groups under multiplication is 1, under addition it is 0.
3. Inverse: For an element $a \in G$, there is the inverse of a (let's say b) that satisfies $a * b = b * a = e$.

Example 1

Example 1

Example

The group $(\mathbb{Z}/n\mathbb{Z}, +)$, which is the set $\{0, 1, 2, \ldots, n-1\}$ under addition taken modulo n, is a group.

Example 1

Example

The group $(\mathbb{Z}/n\mathbb{Z}, +)$, which is the set $\{0, 1, 2, \ldots, n-1\}$ under addition taken modulo n, is a group.

1. This set satisfies associativity because addition is associative. Addition fulfills $(a+b)+c = a+(b+c)$.

Example 1

Example

The group $(\mathbb{Z}/n\mathbb{Z}, +)$, which is the set $\{0, 1, 2, \ldots, n-1\}$ under addition taken modulo n, is a group.

1. This set satisfies associativity because addition is associative. Addition fulfills $(a+b)+c = a+(b+c)$.
2. Identity is 0 because for addition, 0 will always be identity. Identity is any number that produces a for $a+e = e+a$.

Example 1

Example

The group $(\mathbb{Z}/n\mathbb{Z}, +)$, which is the set $\{0, 1, 2, \ldots, n-1\}$ under addition taken modulo n, is a group.

1. This set satisfies associativity because addition is associative. Addition fulfills $(a+b)+c = a+(b+c)$.
2. Identity is 0 because for addition, 0 will always be identity. Identity is any number that produces a for $a+e = e+a$.
3. Inverse of x will be $n-x$.

Example 1

Example

The group $(\mathbb{Z}/n\mathbb{Z}, +)$, which is the set $\{0, 1, 2, \ldots, n-1\}$ under addition taken modulo n, is a group.

1. This set satisfies associativity because addition is associative. Addition fulfills $(a+b)+c = a+(b+c)$.
2. Identity is 0 because for addition, 0 will always be identity. Identity is any number that produces a for $a+e = e+a$.
3. Inverse of x will be $n-x$.

This is an example of a cyclic group, which is a special type of group in which every element can be written as iterated copies of a single element a called a generator of G.

Example 2

Example 2

Example

The set $\mathrm{GL}(2, \mathbb{R})$ of invertible 2×2 real matrices is a group under matrix multiplication.

Example 2

Example

The set $\mathrm{GL}(2, \mathbb{R})$ of invertible 2×2 real matrices is a group under matrix multiplication.

1. Matrix multiplication is associative, so the binary operation here is associative.

Example 2

Example

The set $\mathrm{GL}(2, \mathbb{R})$ of invertible 2×2 real matrices is a group under matrix multiplication.

1. Matrix multiplication is associative, so the binary operation here is associative.
2. The identity matrix is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Example 2

Example

The set $\mathrm{GL}(2, \mathbb{R})$ of invertible 2×2 real matrices is a group under matrix multiplication.

1. Matrix multiplication is associative, so the binary operation here is associative.
2. The identity matrix is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
3. The inverse of the 2×2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is $\frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, which is in $\mathrm{GL}(2, \mathbb{R})$.

Example 3

Example 3

Example

The free group on two elements $\langle a, b \rangle$ consists of all words formed by a, b, a^{-1}, b^{-1}.

Example 3

Example

The free group on two elements $\langle a, b \rangle$ consists of all words formed by a, b, a^{-1}, b^{-1}.

1. It is associative because it is essentially concatenation of words.

Example 3

Example

The free group on two elements $\langle a, b \rangle$ consists of all words formed by a, b, a^{-1}, b^{-1}.

1. It is associative because it is essentially concatenation of words.
2. The identity is the empty word, usually denoted e.

Example 3

Example

The free group on two elements $\langle a, b\rangle$ consists of all words formed by a, b, a^{-1}, b^{-1}.

1. It is associative because it is essentially concatenation of words.
2. The identity is the empty word, usually denoted e.
3. The inverse of every word can be formed by reversing the order and then taking the inverse of each letter.

Example 3

Example

The free group on two elements $\langle a, b \rangle$ consists of all words formed by a, b, a^{-1}, b^{-1}.

1. It is associative because it is essentially concatenation of words.
2. The identity is the empty word, usually denoted e.
3. The inverse of every word can be formed by reversing the order and then taking the inverse of each letter.

*Note that this group is not commutative.

Nonexample 1

Nonexample 1

Non-Example

The set $\mathrm{Mat}_2(\mathbb{R})$ is not a group under multiplication

Nonexample 1

Non-Example

The set $\mathrm{Mat}_2(\mathbb{R})$ is not a group under multiplication

The set is not a group under multiplication because not every matrix has an inverse. For example, $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ does not have a multiplicative inverse because the determinant is 0.

Nonexample 2

Nonexample 2

Non-Example

Integers under multiplication $(\mathbb{Z}, \times)$ are not a group

Nonexample 2

Non-Example

Integers under multiplication $(\mathbb{Z}, \times)$ are not a group

This set is not a group because the inverse does not exist. For instance, there is no inverse of 2 since $1/2$ is not a integer.

Generators and Relations

Free Group

Free Group

Definition

The free group on elements $\langle x_1, x_2, ..., x_n \rangle$ consists of all finite-length words formed by $x_1, x_2, ..., x_n, x_1^{-1}, x_2^{-1}, ..., x_n^{-1}$.

Free Group

Definition

The free group on elements $\langle x_1, x_2, ..., x_n \rangle$ consists of all finite-length words formed by $x_1, x_2, ..., x_n, x_1^{-1}, x_2^{-1}, ..., x_n^{-1}$.

The free group on one element is $\mathbb{Z}$.

Free Group

Definition

The free group on elements $\langle x_1, x_2, ..., x_n \rangle$ consists of all finite-length words formed by $x_1, x_2, ..., x_n, x_1^{-1}, x_2^{-1}, ..., x_n^{-1}$.

The free group on one element is $\mathbb{Z}$.

The free group on two elements was discussed in Example 3.

Generators and Relations

Generators and Relations

Definition

Consider the free group on n elements, $x_1, x_2, ..., x_n$. Let $r_1, r_2, ..., r_m$ be elements in this group (these are just words). The group

$$\langle x_1, x_2, ..., x_n \mid r_1, r_2, ..., r_m \rangle$$

is the quotient we get by setting each r_i equal to identity.

Presentation of a Group

Presentation of a Group

Definition

A presentation of a group, G, is an expression of G in terms of generators and relations (shown in previous slide).

Example 1

Example 1

Example

The group $\mathbb{Z}/3\mathbb{Z}$ has a presentation $\langle x \mid x^3 = e \rangle$.

Example 1

Example

The group $\mathbb{Z}/3\mathbb{Z}$ has a presentation $\langle x \mid x^3 = e \rangle$.

The x represents the element 1, so $x^3 = e$ just means that $1 + 1 + 1 = 0 \pmod 3$.

Example 2

Example 2

Example

The group $\mathbb{Z}^2$ has a presentation $\langle x, y \mid xy = yx \rangle$.

Example 2

Example

The group $\mathbb{Z}^2$ has a presentation $\langle x, y \mid xy = yx \rangle$.

The x and y represent elements $(1, 0)$ and $(0, 1)$, and the relation $xy = yx$ just means that x and y commute.

Example 3

Example 3

Example

The symmetric group S_4 has presentation $\langle x_1, x_2, x_3 \mid x_1^2 = x_2^2 = x_3^2 = (x_1x_2)^3 = (x_2x_3)^3 = e \rangle$.

Example 3

Example

The symmetric group S_4 has presentation $\langle x_1, x_2, x_3 \mid x_1^2 = x_2^2 = x_3^2 = (x_1x_2)^3 = (x_2x_3)^3 = e\rangle$.

The x_i represents the transpositions $(i, i+1)$.

Propositions

Propositions

Proposition

Every group has a presentation.

Propositions

Proposition

Every group has a presentation.

Every group has presentation $\langle \{x_g \mid g \in G\} \mid x_g x_{g'} = x_{gg'} \forall g, g' \in G \rangle$. (Note that the number of generators and relations may be infinite, which is ok).

Propositions

Proposition

Every group has a presentation.

Every group has presentation $\langle \{x_g \mid g \in G\} \mid x_g x_{g'} = x_{gg'} \forall g, g' \in G \rangle$. (Note that the number of generators and relations may be infinite, which is ok).
This is really large to work with by hand, so our examples have much nicer presentations!

Fun problems

Problem 1: Unlooping a rope

Problem 1: Unlooping a rope

Consider two poles that extend infinitely to the sky (and imagine we are living on the $\mathbb{R}^2$ plane).

Problem 1: Unlooping a rope

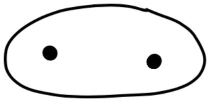
Consider two poles that extend infinitely to the sky (and imagine we are living on the $\mathbb{R}^2$ plane). You want to loop a rope around the two poles and connect the ends such that the rope cannot be removed from the poles.

Problem 1: Unlooping a rope

Consider two poles that extend infinitely to the sky (and imagine we are living on the $\mathbb{R}^2$ plane). You want to loop a rope around the two poles and connect the ends such that the rope cannot be removed from the poles. One simple way to do this is:

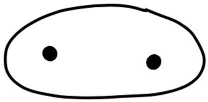
Problem 1: Unlooping a rope

Consider two poles that extend infinitely to the sky (and imagine we are living on the $\mathbb{R}^2$ plane). You want to loop a rope around the two poles and connect the ends such that the rope cannot be removed from the poles. One simple way to do this is:



Problem 1: Unlooping a rope

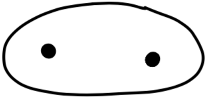
Consider two poles that extend infinitely to the sky (and imagine we are living on the $\mathbb{R}^2$ plane). You want to loop a rope around the two poles and connect the ends such that the rope cannot be removed from the poles. One simple way to do this is:



However, you want to be able to remove the rope by removing either one of the poles. In the picture above, removing a pole does not untangle the rope from the remaining pole.

Problem 1: Unlooping a rope

Consider two poles that extend infinitely to the sky (and imagine we are living on the $\mathbb{R}^2$ plane). You want to loop a rope around the two poles and connect the ends such that the rope cannot be removed from the poles. One simple way to do this is:



However, you want to be able to remove the rope by removing either one of the poles. In the picture above, removing a pole does not untangle the rope from the remaining pole. How can you do it?

Problem 1: Loops as group elements

Problem 1: Loops as group elements

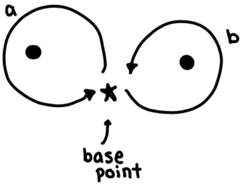
Fix a base point away from the poles.

Problem 1: Loops as group elements

Fix a base point away from the poles.
A loop (beginning and ending at this base point) going counterclockwise around the left pole is denoted as a and a loop going counterclockwise around the right pole is denoted as b.

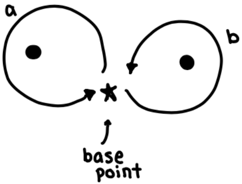
Problem 1: Loops as group elements

Fix a base point away from the poles.
A loop (beginning and ending at this base point) going counterclockwise around the left pole is denoted as a and a loop going counterclockwise around the right pole is denoted as b.



Problem 1: Loops as group elements

Fix a base point away from the poles.
A loop (beginning and ending at this base point) going counterclockwise around the left pole is denoted as a and a loop going counterclockwise around the right pole is denoted as b.



Loops (beginning and ending at the base point, up to homotopy) form a group by concatenation, with inverse being the reverse direction of the loop. This is called the fundamental group: in this case, the group is $\langle a, b \rangle$.

Problem 1: Reformulation in group theory

Problem 1: Reformulation in group theory

A loop is an element of this group $\langle a, b \rangle$.

Problem 1: Reformulation in group theory

A loop is an element of this group $\langle a, b \rangle$.
A loop that is entangled around the poles and cannot be removed is an element that is not the identity.

Problem 1: Reformulation in group theory

A loop is an element of this group $\langle a, b \rangle$.
A loop that is entangled around the poles and cannot be removed is an element that is not the identity.
Removing the left pole is the same as setting a to be the identity element. Similarly, removing the right pole is the same as setting b to be the identity element.

Problem 1: Reformulation in group theory

A loop is an element of this group $\langle a, b \rangle$.
A loop that is entangled around the poles and cannot be removed is an element that is not the identity.
Removing the left pole is the same as setting a to be the identity element. Similarly, removing the right pole is the same as setting b to be the identity element.
We must find an element $x \in \langle a, b \rangle$ that is not identity, but when either a or b is set to identity, x becomes the identity.

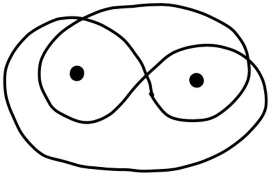
Problem 1: Resolution

Problem 1: Resolution

An element that satisfies these conditions is $aba^{-1}b^{-1}$.

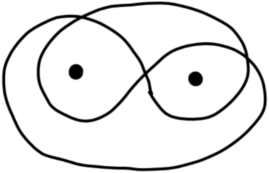
Problem 1: Resolution

An element that satisfies these conditions is $aba^{-1}b^{-1}$.



Problem 1: Resolution

An element that satisfies these conditions is $aba^{-1}b^{-1}$.



Generalization: If instead of 2 poles, there are n poles, can you find a loop which cannot be disentangled, but once any of the n poles are removed, then the loop can be removed?

Problem 1: Resolution

Let $a_1, a_2, \ldots, a_n$ be the generators of the fundamental group, where a_i is the counterclockwise loop around the ith pole.

Problem 1: Resolution

Let $a_1, a_2, \ldots, a_n$ be the generators of the fundamental group, where a_i is the counterclockwise loop around the ith pole.
Let x_{n-1} be the solution representing $n-1$ poles. The element $x_{n-1} a_n x_{n-1}^{-1} a_n^{-1}$ represents the solution for n poles.

Problem 1: Resolution

Let $a_1, a_2, \ldots, a_n$ be the generators of the fundamental group, where a_i is the counterclockwise loop around the ith pole.

Let x_{n-1} be the solution representing $n-1$ poles. The element $x_{n-1}a_nx_{n-1}^{-1}a_n^{-1}$ represents the solution for n poles. Why? When either one of the poles from 1 to $n-1$ are removed, x_{n-1} becomes the identity and the element becomes $a_na_n^{-1}$, which is identity. If the nth pole is removed, the element becomes $x_{n-1}x_{n-1}^{-1}$, which is also identity.

The Alphabet group

The Alphabet group

Let's consider the free group generated by 26 generators, say a,b,c,d,...,x,y,z. Now impose the relations of homophones: that is, for every pair of words which are homophones (i.e. read and red), set them equal (i.e., read=red, where the generators are being multiplied). What is this group?

The Alphabet group

Let's consider the free group generated by 26 generators, say a,b,c,d,...,x,y,z. Now impose the relations of homophones: that is, for every pair of words which are homophones (i.e. read and red), set them equal (i.e., read=red, where the generators are being multiplied). What is this group?
Answer: There are many ways to arrive at the same answer. Here is one plausible solution.

Possible Solutions

Possible Solutions

(1) $by = bye \implies e = 1$

Possible Solutions

(1) $by = bye \implies e = 1$

(2) $see = sea \implies a = 1$

Possible Solutions

(1) $by = bye \implies e = 1$

(2) $see = sea \implies a = 1$

(3) $buy = by \implies u = 1$

Possible Solutions

(1) $by = bye \implies e = 1$

(2) $see = sea \implies a = 1$

(3) $buy = by \implies u = 1$

(4) $fir = fur \implies i = 1$

Possible Solutions

(1) $by = bye \implies e = 1$

(2) $see = sea \implies a = 1$

(3) $buy = by \implies u = 1$

(4) $fir = fur \implies i = 1$

(5) $whole = hole \implies w = 1$

(6) $hour = our \implies h = 1$

(7) $in = inn \implies n = 1$

(8) $knot = not \implies k = 1$

(9) $die = dye \implies y = 1$

(10) $ad = add \implies d = 1$

(11) $all = awl \implies l = 1$

(12) $arc = ark \implies c = 1$

Possible Solutions continued...

Possible Solutions continued...

(13) $ate = eight \implies g = 1$

(14) $base = bass \implies s = 1$

(15) $berry = bury \implies r = 1$

(16) $boos = booze \implies s = 1$

(17) $bat = batt \implies t = 1$

(18) $check = cheque \implies q = 1$

(19) $idle = idol \implies o = 1$

(20) $lam = lamb \implies b = 1$

(21) $coo = coup \implies p = 1$

(22) $faze = phase \implies f = 1$

(23) $genes = jeans \implies j = 1$

(24) $flex = flecks \implies x = 1$

(25) $gamma = gama \implies m = 1$

Explanation of Solution:

Explanation of Solution:

All letters except v are identity. Merriam-Webster finds that there are also no relations in v, so it turns out the quotient group is just $\langle v \rangle \cong \mathbb{Z}$.

Acknowledgements

We would like thank the MIT Math Department, MIT PRIMES, our family, you the audience, and Merrick Cai, our amazing mentor.