Group Theory

Aryaman Maithani

IIT Bombay

23rd July 2020

Greetings

Hi,

Greetings

Hi, welcome to this

Greetings

Hi, welcome to this

group

Greetings

Hi, welcome to this

group discussion.

Greetings

Hi, welcome to this

group discussion.

Credits: Aneesh Bapat

Some examples of groups

Some examples of groups

- The set of real numbers (/complex numbers/rational numbers) along with addition.

Some examples of groups

- The set of real numbers (/complex numbers/rational numbers) along with addition.
- The set of nonzero real numbers (/complex numbers/rational numbers) along with multiplication.

Some examples of groups

- The set of real numbers (/complex numbers/rational numbers) along with addition.
- The set of nonzero real numbers (/complex numbers/rational numbers) along with multiplication.
- The set of integers along with addition.

Some examples of groups

- The set of real numbers (/complex numbers/rational numbers) along with addition.
- The set of nonzero real numbers (/complex numbers/rational numbers) along with multiplication.
- The set of integers along with addition.
- The set of 2×2 invertible real matrices along with multiplication.

Some examples of groups

- The set of real numbers (/complex numbers/rational numbers) along with addition.
- The set of nonzero real numbers (/complex numbers/rational numbers) along with multiplication.
- The set of integers along with addition.
- The set of 2×2 invertible real matrices along with multiplication.
- The set $\{0, 1, \ldots, n-1\}$ along with addition defined modulo n.

Some examples of groups

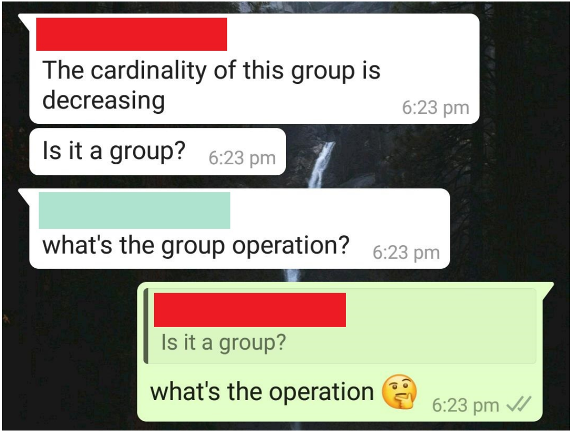
- The set of real numbers (/complex numbers/rational numbers) along with addition.
- The set of nonzero real numbers (/complex numbers/rational numbers) along with multiplication.
- The set of integers along with addition.
- The set of 2×2 invertible real matrices along with multiplication.
- The set $\{0, 1, \ldots, n-1\}$ along with addition defined modulo n.

Some examples of groups

- The set of real numbers (/complex numbers/rational numbers) along with addition.
- The set of nonzero real numbers (/complex numbers/rational numbers) along with multiplication.
- The set of integers along with addition.
- The set of 2×2 invertible real matrices along with multiplication.
- The set $\{0, 1, \ldots, n-1\}$ along with addition defined modulo n.

Note the "along with." We don't talk about a group by just talking about a set. It is necessary to have an operation on it as well.

Joke


[redacted]
The cardinality of this group is decreasing 6:23 pm
Is it a group? 6:23 pm
[redacted]
what's the group operation? 6:23 pm
[redacted]
Is it a group?
what's the operation 6:23 pm

Some non-examples of groups

Some non-examples of groups

- The set of real numbers (/complex numbers/rational numbers) along with multiplication.

Some non-examples of groups

- The set of real numbers (/complex numbers/rational numbers) along with multiplication.
- The set of natural numbers along with addition.

Some non-examples of groups

- The set of real numbers (/complex numbers/rational numbers) along with multiplication.
- The set of natural numbers along with addition.
- The set of non-zero integers (/natural numbers) along with multiplication.

Some non-examples of groups

- The set of real numbers (/complex numbers/rational numbers) along with multiplication.
- The set of natural numbers along with addition.
- The set of non-zero integers (/natural numbers) along with multiplication.
- The set of 2×2 real matrices along with multiplication.

Some non-examples of groups

- The set of real numbers (/complex numbers/rational numbers) along with multiplication.
- The set of natural numbers along with addition.
- The set of non-zero integers (/natural numbers) along with multiplication.
- The set of 2×2 real matrices along with multiplication.
- The set $\{0, 1, \ldots, n-1\}$ with multiplication defined modulo n.

Some non-examples of groups

- The set of real numbers (/complex numbers/rational numbers) along with multiplication.
- The set of natural numbers along with addition.
- The set of non-zero integers (/natural numbers) along with multiplication.
- The set of 2×2 real matrices along with multiplication.
- The set $\{0, 1, \ldots, n-1\}$ with multiplication defined modulo n.
- $\mathbb{R}^3$ with cross-product.

Some non-examples of groups

- The set of real numbers (/complex numbers/rational numbers) along with multiplication.
- The set of natural numbers along with addition.
- The set of non-zero integers (/natural numbers) along with multiplication.
- The set of 2×2 real matrices along with multiplication.
- The set $\{0, 1, \ldots, n-1\}$ with multiplication defined modulo n.
- $\mathbb{R}^3$ with cross-product.
- Empty set with the empty operation.

What is a group?

Hmmmmmmmmmmmmmmmmm?

What is a group?

First, a definition.

Definition 1 (Binary operation)

Given a set S, a binary operation $\cdot$ on S is a function of the form

$$\cdot : S \times S \to S.$$

What is a group?

Definition 1 (Binary operation)

Given a set S, a binary operation $\cdot$ on S is a function of the form

$$\cdot : S \times S \to S.$$

For ease of notation, we shall write $a \cdot b$ instead of $\cdot((a, b))$.

What is a group?

Definition 1 (Binary operation)

Given a set S, a binary operation $\cdot$ on S is a function of the form

$$\cdot : S \times S \to S.$$

For ease of notation, we shall write $a \cdot b$ instead of $\cdot((a, b))$.
Examples?

What is a group?

Definition 1 (Binary operation)

Given a set S, a binary operation $\cdot$ on S is a function of the form

$$\cdot : S \times S \to S.$$

For ease of notation, we shall write $a \cdot b$ instead of $\cdot((a, b))$.

What is a group?

Definition 1 (Binary operation)

Given a set S, a binary operation $\cdot$ on S is a function of the form

$$\cdot : S \times S \to S.$$

For ease of notation, we shall write $a \cdot b$ instead of $\cdot((a, b))$.

- $+$ and $\cdot$ are binary operations on $\mathbb{R}(/\mathbb{Q}/\mathbb{C}/\mathbb{Z})$.

What is a group?

Definition 1 (Binary operation)

Given a set S, a binary operation $\cdot$ on S is a function of the form

$$\cdot : S \times S \to S.$$

For ease of notation, we shall write $a \cdot b$ instead of $\cdot((a, b))$.

- $+$ and $\cdot$ are binary operations on $\mathbb{R}(/\mathbb{Q}/\mathbb{C}/\mathbb{Z})$.
- $-$ is also a binary operation on the above sets but $\div$ is not.

What is a group?

Definition 1 (Binary operation)

Given a set S, a binary operation $\cdot$ on S is a function of the form

$$\cdot : S \times S \to S.$$

For ease of notation, we shall write $a \cdot b$ instead of $\cdot((a, b))$.

- $+$ and $\cdot$ are binary operations on $\mathbb{R}(/\mathbb{Q}/\mathbb{C}/\mathbb{Z})$.
- $-$ is also a binary operation on the above sets but $\div$ is not.
- $+$ is a binary operation on $\mathbb{N}$ but $-$ is not.

What is a group?

Definition 1 (Binary operation)

Given a set S, a binary operation $\cdot$ on S is a function of the form

$$\cdot : S \times S \to S.$$

For ease of notation, we shall write $a \cdot b$ instead of $\cdot((a, b))$.

- $+$ and $\cdot$ are binary operations on $\mathbb{R}(/\mathbb{Q}/\mathbb{C}/\mathbb{Z})$.
- $-$ is also a binary operation on the above sets but $\div$ is not.
- $+$ is a binary operation on $\mathbb{N}$ but $-$ is not.
- $+$ and $\cdot$ modulo n are binary operations on $\{0, \ldots, n-1\}$.

What is a group?

Definition 1 (Binary operation)

Given a set S, a binary operation $\cdot$ on S is a function of the form

$$\cdot : S \times S \to S.$$

For ease of notation, we shall write $a \cdot b$ instead of $\cdot((a, b))$.

- $+$ and $\cdot$ are binary operations on $\mathbb{R}(/\mathbb{Q}/\mathbb{C}/\mathbb{Z})$.
- $-$ is also a binary operation on the above sets but $\div$ is not.
- $+$ is a binary operation on $\mathbb{N}$ but $-$ is not.
- $+$ and $\cdot$ modulo n are binary operations on $\{0, \ldots, n-1\}$.
- $\times$ (cross product) is a binary operation on $\mathbb{R}^3$.

What is a group?

Definition 1 (Binary operation)

Given a set S, a binary operation $\cdot$ on S is a function of the form

$$\cdot : S \times S \to S.$$

For ease of notation, we shall write $a \cdot b$ instead of $\cdot((a, b))$.

- $+$ and $\cdot$ are binary operations on $\mathbb{R}(/\mathbb{Q}/\mathbb{C}/\mathbb{Z})$.
- $-$ is also a binary operation on the above sets but $\div$ is not.
- $+$ is a binary operation on $\mathbb{N}$ but $-$ is not.
- $+$ and $\cdot$ modulo n are binary operations on $\{0, \ldots, n-1\}$.
- $\times$ (cross product) is a binary operation on $\mathbb{R}^3$.

Now, we define what a group is.

What is a group?

Definition 2 (Group)

A group is an ordered pair $(G, \cdot)$ where G is some set and $\cdot$ is a binary operation on G satisfying the following axioms:

What is a group?

Definition 2 (Group)

A group is an ordered pair $(G, \cdot)$ where G is some set and $\cdot$ is a binary operation on G satisfying the following axioms:

1. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in G$,

What is a group?

Definition 2 (Group)

A group is an ordered pair $(G, \cdot)$ where G is some set and $\cdot$ is a binary operation on G satisfying the following axioms:

1. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in G$,
2. there exists an element e in G, called an *identity* of G, such that for all $a \in G$ we have $a \cdot e = a = a \cdot e$,

What is a group?

Definition 2 (Group)

A group is an ordered pair $(G, \cdot)$ where G is some set and $\cdot$ is a binary operation on G satisfying the following axioms:

1. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in G$,
2. there exists an element e in G, called an *identity* of G, such that for all $a \in G$ we have $a \cdot e = a = a \cdot e$,
3. for each $a \in G$, there is an element $a^{-1} \in G$, called an *inverse* of a such that $a \cdot a^{-1} = e = a^{-1} \cdot a$.

What is a group?

Definition 2 (Group)

A group is an ordered pair $(G, \cdot)$ where G is some set and $\cdot$ is a binary operation on G satisfying the following axioms:

1. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in G$,
2. there exists an element e in G, called an *identity* of G, such that for all $a \in G$ we have $a \cdot e = a = a \cdot e$,
3. for each $a \in G$, there is an element $a^{-1} \in G$, called an *inverse* of a such that $a \cdot a^{-1} = e = a^{-1} \cdot a$.

What is a group?

Definition 2 (Group)

A group is an ordered pair $(G, \cdot)$ where G is some set and $\cdot$ is a binary operation on G satisfying the following axioms:

1. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in G$,
2. there exists an element e in G, called an *identity* of G, such that for all $a \in G$ we have $a \cdot e = a = a \cdot e$,
3. for each $a \in G$, there is an element $a^{-1} \in G$, called an *inverse* of a such that $a \cdot a^{-1} = e = a^{-1} \cdot a$.

I have used "an" above. Why?

What is a group?

Definition 2 (Group)

A group is an ordered pair $(G, \cdot)$ where G is some set and $\cdot$ is a binary operation on G satisfying the following axioms:

1. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in G$,
2. there exists an element e in G, called an *identity* of G, such that for all $a \in G$ we have $a \cdot e = a = a \cdot e$,
3. for each $a \in G$, there is an element $a^{-1} \in G$, called an *inverse* of a such that $a \cdot a^{-1} = e = a^{-1} \cdot a$.

I have used "an" above. Why? Well, simply because I can't directly claim that identity (/inverse) is unique. However, it is.

Definition 2 (Group)

A group is an ordered pair $(G, \cdot)$ where G is some set and $\cdot$ is a binary operation on G satisfying the following axioms:

1. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in G$,
2. there exists an element e in G, called an *identity* of G, such that for all $a \in G$ we have $a \cdot e = a = a \cdot e$,
3. for each $a \in G$, there is an element $a^{-1} \in G$, called an *inverse* of a such that $a \cdot a^{-1} = e = a^{-1} \cdot a$.

I have used "an" above. Why? Well, simply because I can't directly claim that identity (/inverse) is unique. However, it is.

Proof?

Review

The discussion we had is what led to us agreeing upon the above axioms. So, let us only discuss what went wrong with the non-examples.

Review

- The set of real numbers (/complex numbers/rational numbers) along with multiplication.

Review

- The set of real numbers (/complex numbers/rational numbers) along with multiplication.
- The set of natural numbers along with addition.

Review

- The set of real numbers (/complex numbers/rational numbers) along with multiplication.
- The set of natural numbers along with addition.
- The set of non-zero integers (/natural numbers) along with multiplication.

Review

- The set of real numbers (/complex numbers/rational numbers) along with multiplication.
- The set of natural numbers along with addition.
- The set of non-zero integers (/natural numbers) along with multiplication.
- The set of 2×2 real matrices along with multiplication.

Review

- The set of real numbers (/complex numbers/rational numbers) along with multiplication.
- The set of natural numbers along with addition.
- The set of non-zero integers (/natural numbers) along with multiplication.
- The set of 2×2 real matrices along with multiplication.
- The set $\{0, 1, \ldots, n-1\}$ with multiplication defined modulo n.

Review

- The set of real numbers (/complex numbers/rational numbers) along with multiplication.
- The set of natural numbers along with addition.
- The set of non-zero integers (/natural numbers) along with multiplication.
- The set of 2×2 real matrices along with multiplication.
- The set $\{0, 1, \ldots, n-1\}$ with multiplication defined modulo n.
- $\mathbb{R}^3$ with cross-product.

Review

- The set of real numbers (/complex numbers/rational numbers) along with multiplication.
- The set of natural numbers along with addition.
- The set of non-zero integers (/natural numbers) along with multiplication.
- The set of 2×2 real matrices along with multiplication.
- The set $\{0, 1, \ldots, n-1\}$ with multiplication defined modulo n.
- $\mathbb{R}^3$ with cross-product.
- Empty set with the empty operation.

Review

- The set of real numbers (/complex numbers/rational numbers) along with multiplication.
- The set of natural numbers along with addition.
- The set of non-zero integers (/natural numbers) along with multiplication.
- The set of 2×2 real matrices along with multiplication.
- The set $\{0, 1, \ldots, n-1\}$ with multiplication defined modulo n.
- $\mathbb{R}^3$ with cross-product.
- Empty set with the empty operation.

Note that we need the set to be nonempty since it must always have the identity.

Review

- The set of real numbers (/complex numbers/rational numbers) along with multiplication.
- The set of natural numbers along with addition.
- The set of non-zero integers (/natural numbers) along with multiplication.
- The set of 2×2 real matrices along with multiplication.
- The set $\{0, 1, \ldots, n-1\}$ with multiplication defined modulo n.
- $\mathbb{R}^3$ with cross-product.
- Empty set with the empty operation.

Note that we need the set to be nonempty since it must always have the identity.

Recall vector spaces?

Review

- The set of real numbers (/complex numbers/rational numbers) along with multiplication.
- The set of natural numbers along with addition.
- The set of non-zero integers (/natural numbers) along with multiplication.
- The set of 2×2 real matrices along with multiplication.
- The set $\{0, 1, \ldots, n-1\}$ with multiplication defined modulo n.
- $\mathbb{R}^3$ with cross-product.
- Empty set with the empty operation.

Note that we need the set to be nonempty since it must always have the identity.

Recall vector spaces? Verify that any vector space along with its $+$ forms a group.

Abelian groups

Commutativity

Abelian groups

Commutativity... is nice.

Abelian groups

Commutativity… is nice.
Due to this, commutative groups have a name of their own.

Abelian groups

Commutativity... is nice.
Due to this, commutative groups have a name of their own.

Definition 3 (Abelian groups)

A group $(G, \cdot)$ is said to be abelian if

$$a \cdot b = b \cdot a$$

for all $a, b \in G$.

Abelian groups

Commutativity... is nice.
Due to this, commutative groups have a name of their own.

Definition 3 (Abelian groups)

A group $(G, \cdot)$ is said to be abelian if

$$a \cdot b = b \cdot a$$

for all $a, b \in G$.

From the second slide, everything except for the matrix example was an example of an abelian.

Abelian groups

Commutativity... is nice.
Due to this, commutative groups have a name of their own.

Definition 3 (Abelian groups)

A group $(G, \cdot)$ is said to be abelian if

$$a \cdot b = b \cdot a$$

for all $a, b \in G$.

From the second slide, everything except for the matrix example was an example of an abelian.
Even the example of $(V, +)$ for a vector space V is an abelian group.

Abelian groups

Commutativity... is nice.
Due to this, commutative groups have a name of their own.

Definition 3 (Abelian groups)

A group $(G, \cdot)$ is said to be abelian if

$$a \cdot b = b \cdot a$$

for all $a, b \in G$.

From the second slide, everything except for the matrix example was an example of an abelian.
Even the example of $(V, +)$ for a vector space V is an abelian group.

Abelian groups are named after early 19th century mathematician Niels Henrik Abel.

Abelian groups

Commutativity... is nice.
Due to this, commutative groups have a name of their own.

Definition 3 (Abelian groups)

A group $(G, \cdot)$ is said to be abelian if

$$a \cdot b = b \cdot a$$

for all $a, b \in G$.

From the second slide, everything except for the matrix example was an example of an abelian.
Even the example of $(V, +)$ for a vector space V is an abelian group.

Abelian groups are named after early 19th century mathematician Niels Henrik Abel.

Abuse of notation

It is a common theme in math to abuse notation.

Abuse of notation

It is a common theme in math to abuse notation.
Following this theme, we note that instead of writing "$(G, \cdot)$ is a group," we often write the following:

Abuse of notation

It is a common theme in math to abuse notation.
Following this theme, we note that instead of writing "$(G, \cdot)$ is a group," we often write the following:

- "G is a group under $\cdot$," or

Abuse of notation

It is a common theme in math to abuse notation.
Following this theme, we note that instead of writing "$(G, \cdot)$ is a group," we often write the following:

- "G is a group under $\cdot$," or
- "G is a group" when $\cdot$ is clear from context.

Notations

Let G be a group and $x \in G$. We define x^n for $n \in \mathbb{Z}$ as follows:

$x^0 :=$

For $n > 0$, we define

$$x^n :=$$

For $n < 0$, we have $x^n :=$, which is the same as (Prove!)

Notations

Let G be a group and $x \in G$. We define x^n for $n \in \mathbb{Z}$ as follows:

$x^0 := e$.
For $n > 0$, we define

$$x^n :=$$

For $n < 0$, we have $x^n :=$, which is the same as
(Prove!)

Notations

Let G be a group and $x \in G$. We define x^n for $n \in \mathbb{Z}$ as follows:

$x^0 := e$.
For $n > 0$, we define

$$x^n := \underbrace{x \cdot x \cdots x}_{n \text{ times}}.$$

For $n < 0$, we have $x^n :=$, which is the same as
(Prove!)

Notations

Let G be a group and $x \in G$. We define x^n for $n \in \mathbb{Z}$ as follows:

$x^0 := e$.
For $n > 0$, we define

$$x^n := \underbrace{x \cdot x \cdots x}_{n \text{ times}}.$$

For $n < 0$, we have $x^n := (x^{-1})^{-n}$, which is the same as
(Prove!)

Notations

Let G be a group and $x \in G$. We define x^n for $n \in \mathbb{Z}$ as follows:

$x^0 := e$.
For $n > 0$, we define

$$x^n := \underbrace{x \cdot x \cdots x}_{n \text{ times}}.$$

For $n < 0$, we have $x^n := (x^{-1})^{-n}$, which is the same as $(x^{-n})^{-1}$. (Prove!)

Orders

Orders

Definition 4 (Order (group))

The order of a group is the cardinality of G.
It is denoted by $|G|$.

Orders

Definition 4 (Order (group))

The order of a group is the cardinality of G.
It is denoted by $|G|$.

Note that the order of a group may be infinite. A group is said to be finite if its cardinality is.

Orders

Definition 4 (Order (group))

The order of a group is the cardinality of G.
It is denoted by $|G|$.

Note that the order of a group may be infinite. A group is said to be finite if its cardinality is.

Definition 5 (Order (element))

The order of an element $x \in G$ the smallest positiver integer n such that

$$x^n = e.$$

(Where e is the identity of G.)
If no such n exists, then we say the the element has infinite order.
It is denoted by $|x|$.

Finite groups

Proposition 1

Every element of a finite group has finite order.

Finite groups

Proposition 1

Every element of a finite group has finite order.

Proof.

Let G be a finite group and let $x \in G$.
It suffices to show that $x^n = e$ for *some* $n \in \mathbb{N}$.
Note that $x^0, x^1, \ldots, x^{|G|}$ are $|G| + 1$ elements of G. By PHP, two of them must be equal. Thus,

$$x^n = x^m$$

for some $0 \leq n < m \leq |G|$.
The above equation gives us

$$e = x^{m-n}.$$

Since $m - n \in \mathbb{N}$, we are done. □

Subgroups

What we shall see now is a recurring theme in mathematics.

Subgroups

What we shall see now is a recurring theme in mathematics. Given a set with some certain properties, we look at subsets which have the same properties.

What we shall see now is a recurring theme in mathematics.
Given a set with some certain properties, we look at subsets which have the same properties.
Where have you seen this before?

Subgroups

What we shall see now is a recurring theme in mathematics.
Given a set with some certain properties, we look at subsets which have the same properties.
Where have you seen this before?
There are many examples:

- Subspaces of vector spaces,

Subgroups

What we shall see now is a recurring theme in mathematics.
Given a set with some certain properties, we look at subsets which have the same properties.
Where have you seen this before?
There are many examples:

- Subspaces of vector spaces,
- Subgroups of groups,

Subgroups

What we shall see now is a recurring theme in mathematics.
Given a set with some certain properties, we look at subsets which have the same properties.
Where have you seen this before?
There are many examples:

- Subspaces of vector spaces,
- Subgroups of groups,
- Subrings of rings,

Subgroups

What we shall see now is a recurring theme in mathematics.
Given a set with some certain properties, we look at subsets which have the same properties.
Where have you seen this before?
There are many examples:

- Subspaces of vector spaces,
- Subgroups of groups,
- Subrings of rings,
- Subfields of fields,

Subgroups

What we shall see now is a recurring theme in mathematics.
Given a set with some certain properties, we look at subsets which have the same properties.
Where have you seen this before?
There are many examples:

- Subspaces of vector spaces,
- Subgroups of groups,
- Subrings of rings,
- Subfields of fields,
- Subspaces of (metric/topological) spaces, et cetera.

Subgroups

The idea is to find a subset of G which can be regarded as a group in its own right.

Subgroups

The idea is to find a subset of G which can be regarded as a group in its own right. What group operation should we give it then?

Subgroups

The idea is to find a subset of G which can be regarded as a group in its own right. What group operation should we give it then? Well, it is natural to consider the same operation as that of G.

Subgroups

The idea is to find a subset of G which can be regarded as a group in its own right. What group operation should we give it then? Well, it is natural to consider the same operation as that of G.

Definition 6 (Subgroup)

A subset $H \subset G$ is said to be *subgroup* of G if:

Subgroups

The idea is to find a subset of G which can be regarded as a group in its own right. What group operation should we give it then? Well, it is natural to consider the same operation as that of G.

Definition 6 (Subgroup)

A subset $H \subset G$ is said to be *subgroup* of G if:

- H is nonempty.

Subgroups

The idea is to find a subset of G which can be regarded as a group in its own right. What group operation should we give it then? Well, it is natural to consider the same operation as that of G.

Definition 6 (Subgroup)

A subset $H \subset G$ is said to be *subgroup* of G if:

- H is nonempty.
- $a \cdot b \in H$ for all $a, b \in H$,

Subgroups

The idea is to find a subset of G which can be regarded as a group in its own right. What group operation should we give it then? Well, it is natural to consider the same operation as that of G.

Definition 6 (Subgroup)

A subset $H \subset G$ is said to be *subgroup* of G if:

- H is nonempty.
- $a \cdot b \in H$ for all $a, b \in H$,
- $a^{-1} \in H$ for all $a \in H$.

Subgroups

The idea is to find a subset of G which can be regarded as a group in its own right. What group operation should we give it then? Well, it is natural to consider the same operation as that of G.

Definition 6 (Subgroup)

A subset $H \subset G$ is said to be *subgroup* of G if:

- H is nonempty.
- $a \cdot b \in H$ for all $a, b \in H$,
- $a^{-1} \in H$ for all $a \in H$.

The above conditions just tell us that $\cdot$ (restricted to H) is a binary operation on H and that $(H, \cdot|_H)$ forms a group.

Subgroups

The idea is to find a subset of G which can be regarded as a group in its own right. What group operation should we give it then? Well, it is natural to consider the same operation as that of G.

Definition 6 (Subgroup)

A subset $H \subset G$ is said to be *subgroup* of G if:

- H is nonempty.
- $a \cdot b \in H$ for all $a, b \in H$,
- $a^{-1} \in H$ for all $a \in H$.

The above conditions just tell us that $\cdot$ (restricted to H) is a binary operation on H and that $(H, \cdot|_H)$ forms a group.

One may note that the identity element of $(G, \cdot)$ is always present in H and moreover, it is also the identity of $(H, \cdot|_H)$.

Examples

Notation: If H is a subgroup of G, then we write $H \leq G$.

Examples

Notation: If H is a subgroup of G, then we write $H \leq G$.

- A group always has at least two subgroups. Can you tell which?

Examples

Notation: If H is a subgroup of G, then we write $H \leq G$.

- A group always has at least two subgroups. Can you tell which? (Well, not two if G has only one element.)
- Is $\mathbb{N} \leq \mathbb{Z}$?

Examples

Notation: If H is a subgroup of G, then we write $H \leq G$.

- A group always has at least two subgroups. Can you tell which? (Well, not two if G has only one element.)
- Is $\mathbb{N} \leq \mathbb{Z}$?
- Is $n\mathbb{Z} \leq \mathbb{Z}$?

Examples

Notation: If H is a subgroup of G, then we write $H \leq G$.

- A group always has at least two subgroups. Can you tell which? (Well, not two if G has only one element.)
- Is $\mathbb{N} \leq \mathbb{Z}$?
- Is $n\mathbb{Z} \leq \mathbb{Z}$? In fact, any subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$.

Examples

Notation: If H is a subgroup of G, then we write $H \leq G$.

- A group always has at least two subgroups. Can you tell which? (Well, not two if G has only one element.)
- Is $\mathbb{N} \leq \mathbb{Z}$?
- Is $n\mathbb{Z} \leq \mathbb{Z}$? In fact, any subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$.
- $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.

Examples

Notation: If H is a subgroup of G, then we write $H \leq G$.

- A group always has at least two subgroups. Can you tell which? (Well, not two if G has only one element.)
- Is $\mathbb{N} \leq \mathbb{Z}$?
- Is $n\mathbb{Z} \leq \mathbb{Z}$? In fact, any subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$.
- $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.
- The set of $n \times n$ invertible upper triangular (real) matrices is a subgroup of the group of all invertible $n \times n$ (real) matrices.

Cosets

Let H be a subgroup of G.

Cosets

Let H be a subgroup of G. For $g \in G$, we define $g \cdot H$ as

$$g \cdot H := \{g \cdot h : h \in H\}.$$

Cosets

Let H be a subgroup of G. For $g \in G$, we define $g \cdot H$ as

$$g \cdot H := \{g \cdot h : h \in H\}.$$

Definition 7 (Coset)

A *(left) coset* of H is a set of the form $g \cdot H$.

g is said to be a representative of the coset $g \cdot H$.

Let H be a subgroup of G. For $g \in G$, we define $g \cdot H$ as

$$g \cdot H := \{g \cdot h : h \in H\}.$$

Definition 7 (Coset)

A *(left) coset* of H is a set of the form $g \cdot H$.

g is said to be a representative of the coset $g \cdot H$.
We define G/H be the set of cosets, that is,

$$G/H := \{gH : g \in G\}.$$

Let H be a subgroup of G. For $g \in G$, we define $g \cdot H$ as

$$g \cdot H := \{g \cdot h : h \in H\}.$$

Definition 7 (Coset)

A *(left) coset* of H is a set of the form $g \cdot H$.

g is said to be a representative of the coset $g \cdot H$.
We define G/H be the set of cosets, that is,

$$G/H := \{gH : g \in G\}.$$

Note that different elements could correspond to the same coset. That is, a coset may have different representatives.

Let H be a subgroup of G. For $g \in G$, we define $g \cdot H$ as

$$g \cdot H := \{g \cdot h : h \in H\}.$$

Definition 7 (Coset)

A *(left) coset* of H is a set of the form $g \cdot H$.

g is said to be a representative of the coset $g \cdot H$.
We define G/H be the set of cosets, that is,

$$G/H := \{gH : g \in G\}.$$

Note that different elements could correspond to the same coset. That is, a coset may have different representatives. In fact, we now see precisely when that is possible.

Properties of cosets

Proposition 2 (Equality of cosets)

Let $a, b \in G$. Then,

$$aH = bH \quad \text{iff} \quad b^{-1}aH = H \quad \text{iff} \quad b^{-1}a \in H.$$

Proposition 2 (Equality of cosets)

Let $a, b \in G$. Then,

$$aH = bH \quad \text{iff} \quad b^{-1}aH = H \quad \text{iff} \quad b^{-1}a \in H.$$

This tells us that if $c \in aH$, then $aH = cH$.

Proposition 2 (Equality of cosets)

Let $a, b \in G$. Then,

$$aH = bH \quad \text{iff} \quad b^{-1}aH = H \quad \text{iff} \quad b^{-1}a \in H.$$

This tells us that if $c \in aH$, then $aH = cH$. This also leads to the following result.

Proposition 2 (Equality of cosets)

Let $a, b \in G$. Then,

$$aH = bH \quad \text{iff} \quad b^{-1}aH = H \quad \text{iff} \quad b^{-1}a \in H.$$

This tells us that if $c \in aH$, then $aH = cH$. This also leads to the following result.

Proposition 3 (Disjointness of cosets)

If aH and bH are two cosets, then either they are equal or they are disjoint.

Properties of cosets

Proposition 2 (Equality of cosets)

Let $a, b \in G$. Then,

$$aH = bH \quad \text{iff} \quad b^{-1}aH = H \quad \text{iff} \quad b^{-1}a \in H.$$

This tells us that if $c \in aH$, then $aH = cH$. This also leads to the following result.

Proposition 3 (Disjointness of cosets)

If aH and bH are two cosets, then either they are equal or they are disjoint.

Note that H itself is a coset since it equals $e \cdot H$. (Or $h \cdot H$ for any $h \in H$.)

Proposition 4 (Equality of cardinalities)

Given any coset aH, it has the same cardinality as H.

Properties of cosets

Proposition 4 (Equality of cardinalities)

Given any coset aH, it has the same cardinality as H.

(That is, there is a bijection between aH and H.)

Proposition 4 (Equality of cardinalities)

Given any coset aH, it has the same cardinality as H.

(That is, there is a bijection between aH and H.)

Proof.

Consider the function $f : H \to aH$ defined by

$$f(h) = a \cdot h.$$

□

Proposition 4 (Equality of cardinalities)

Given any coset aH, it has the same cardinality as H.

(That is, there is a bijection between aH and H.)

Proof.

Consider the function $f : H \to aH$ defined by

$$f(h) = a \cdot h.$$

This is clearly onto, by definition of aH.

□

Proposition 4 (Equality of cardinalities)

Given any coset aH, it has the same cardinality as H.

(That is, there is a bijection between aH and H.)

Proof.

Consider the function $f : H \to aH$ defined by

$$f(h) = a \cdot h.$$

This is clearly onto, by definition of aH.
Moreover, this is one-one since $ah = ah' \implies h = h'$.

□

Properties of cosets

Proposition 4 (Equality of cardinalities)

Given any coset aH, it has the same cardinality as H.

(That is, there is a bijection between aH and H.)

Proof.

Consider the function $f : H \to aH$ defined by

$$f(h) = a \cdot h.$$

This is clearly onto, by definition of aH.
Moreover, this is one-one since $ah = ah' \implies h = h'$. (One can cancel a since it has an inverse.) □

Properties of cosets

Proposition 4 (Equality of cardinalities)

Given any coset aH, it has the same cardinality as H.

(That is, there is a bijection between aH and H.)

Proof.

Consider the function $f : H \to aH$ defined by

$$f(h) = a \cdot h.$$

This is clearly onto, by definition of aH.
Moreover, this is one-one since $ah = ah' \implies h = h'$. (One can cancel a since it has an inverse.) $\square$

Remark. This shows that any two cosets have the same cardinality.

Lagrange's Theorem

With the concept of cosets, we can prove a (quite fundamental) result of group theory.

Lagrange's Theorem

Theorem 1 (Lagrange's Theorem)

Let G be a finite group and $H \leq G$.
Then, $|H|$ divides $|G|$.

Theorem 1 (Lagrange's Theorem)

Let G be a finite group and $H \leq G$.
Then, $|H|$ divides $|G|$.

Proof.

$\square$

Lagrange's Theorem

Theorem 1 (Lagrange's Theorem)

Let G be a finite group and $H \leq G$.
Then, $|H|$ divides $|G|$.

Proof.

Left as an exercise to the reader. □

Lagrange's Theorem

Theorem 1 (Lagrange's Theorem)

Let G be a finite group and $H \leq G$.
Then, $|H|$ divides $|G|$.

Proof.

Jk. □

Lagrange's Theorem

Theorem 1 (Lagrange's Theorem)

Let G be a finite group and $H \leq G$.
Then, $|H|$ divides $|G|$.

Proof.

Consider the set of cosets $G/H = \{a_1 H, \ldots, a_n H\}$.

□

Lagrange's Theorem

Theorem 1 (Lagrange's Theorem)

Let G be a finite group and $H \leq G$.
Then, $|H|$ divides $|G|$.

Proof.

Consider the set of cosets $G/H = \{a_1H, \ldots, a_nH\}$.
Note that given any element $g \in G$, it must belong to *some* coset.
(Why?)

□

Lagrange's Theorem

Theorem 1 (Lagrange's Theorem)

Let G be a finite group and $H \leq G$.
Then, $|H|$ divides $|G|$.

Proof.

Consider the set of cosets $G/H = \{a_1H, \ldots, a_nH\}$.
Note that given any element $g \in G$, it must belong to *some* coset. (Why?)
Thus, $G = a_1H \cup \cdots \cup a_nH$.

□

Lagrange's Theorem

Theorem 1 (Lagrange's Theorem)

Let G be a finite group and $H \leq G$.
Then, $|H|$ divides $|G|$.

Proof.

Consider the set of cosets $G/H = \{a_1H, \ldots, a_nH\}$.
Note that given any element $g \in G$, it must belong to *some* coset. (Why?)
Thus, $G = a_1H \cup \cdots \cup a_nH$.
Moreover, by our previous observation, the above union is of disjoint sets. Thus,

□

Theorem 1 (Lagrange's Theorem)

Let G be a finite group and $H \leq G$.
Then, $|H|$ divides $|G|$.

Proof.

Consider the set of cosets $G/H = \{a_1H, \ldots, a_nH\}$.
Note that given any element $g \in G$, it must belong to *some* coset. (Why?)
Thus, $G = a_1H \cup \cdots \cup a_nH$.
Moreover, by our previous observation, the above union is of disjoint sets. Thus,

$$|G| = |a_1H| + \cdots + |a_nH|$$

□

Lagrange's Theorem

Theorem 1 (Lagrange's Theorem)

Let G be a finite group and $H \leq G$.
Then, $|H|$ divides $|G|$.

Proof.

Consider the set of cosets $G/H = \{a_1H, \ldots, a_nH\}$.
Note that given any element $g \in G$, it must belong to *some* coset. (Why?)
Thus, $G = a_1H \cup \cdots \cup a_nH$.
Moreover, by our previous observation, the above union is of disjoint sets. Thus,

$$\begin{aligned} |G| &= |a_1H| + \cdots + |a_nH| \\ &= n|H|. \end{aligned}$$

□

Lagrange's Theorem

Theorem 1 (Lagrange's Theorem)

Let G be a finite group and $H \leq G$.
Then, $|H|$ divides $|G|$.

Proof.

Consider the set of cosets $G/H = \{a_1 H, \ldots, a_n H\}$.
Note that given any element $g \in G$, it must belong to *some* coset. (Why?)
Thus, $G = a_1 H \cup \cdots \cup a_n H$.
Moreover, by our previous observation, the above union is of disjoint sets. Thus,

$$\begin{aligned} |G| &= |a_1 H| + \cdots + |a_n H| \\ &= n|H|. \end{aligned}$$

That completes our proof. □

Homomorphisms

What we consider now is another common theme in mathematics.

Homomorphisms

What we consider now is another common theme in mathematics. Given two objects of the same type (for example, given two groups), we consider functions between them.

Homomorphisms

What we consider now is another common theme in mathematics. Given two objects of the same type (for example, given two groups), we consider functions between them. However, we don't just consider any function. We study some particular type of functions.

Homomorphisms

What we consider now is another common theme in mathematics. Given two objects of the same type (for example, given two groups), we consider functions between them. However, we don't just consider any function. We study some particular type of functions.

Do you recall what particular type of functions (between vector spaces) we considered in linear algebra?

Homomorphisms

What we consider now is another common theme in mathematics. Given two objects of the same type (for example, given two groups), we consider functions between them. However, we don't just consider any function. We study some particular type of functions.

Do you recall what particular type of functions (between vector spaces) we considered in linear algebra?
Similar to that, we consider functions that preserve the "structure" of the objects in consideration.

Homomorphisms

What we consider now is another common theme in mathematics. Given two objects of the same type (for example, given two groups), we consider functions between them. However, we don't just consider any function. We study some particular type of functions.

Do you recall what particular type of functions (between vector spaces) we considered in linear algebra?
Similar to that, we consider functions that preserve the "structure" of the objects in consideration.

The case of groups is particularly simple since there's pretty one much thing that gives the group its structure, the group operation.

Homomorphisms

What we consider now is another common theme in mathematics. Given two objects of the same type (for example, given two groups), we consider functions between them. However, we don't just consider any function. We study some particular type of functions.

Do you recall what particular type of functions (between vector spaces) we considered in linear algebra?
Similar to that, we consider functions that preserve the "structure" of the objects in consideration.

The case of groups is particularly simple since there's pretty one much thing that gives the group its structure, the group operation. This leads to the following definition.

Homomorphisms

Definition 8 (Homomorphism)

Let $(G, \cdot)$ and $(H, \star)$ be groups. A function

$$\varphi : G \to H$$

is said to be a *group homomorphism* if

$$\varphi(a \cdot b) = \varphi(a) \star \varphi(b)$$

for all $a, b \in G$.

Homomorphisms

Definition 8 (Homomorphism)

Let $(G, \cdot)$ and $(H, \star)$ be groups. A function

$$\varphi : G \to H$$

is said to be a *group homomorphism* if

$$\varphi(a \cdot b) = \varphi(a) \star \varphi(b)$$

for all $a, b \in G$.

One checks the following properties easily:

Definition 8 (Homomorphism)

Let $(G, \cdot)$ and $(H, \star)$ be groups. A function

$$\varphi : G \to H$$

is said to be a *group homomorphism* if

$$\varphi(a \cdot b) = \varphi(a) \star \varphi(b)$$

for all $a, b \in G$.

One checks the following properties easily:

- $\varphi(e_G) = e_H$,

Definition 8 (Homomorphism)

Let $(G, \cdot)$ and $(H, \star)$ be groups. A function

$$\varphi : G \to H$$

is said to be a *group homomorphism* if

$$\varphi(a \cdot b) = \varphi(a) \star \varphi(b)$$

for all $a, b \in G$.

One checks the following properties easily:

- $\varphi(e_G) = e_H$,
- $\varphi(a^{-1}) = (\varphi(a))^{-1}$ for all $a \in G$.

Properties of homomorphisms

Now, we see some properties of homomorphisms themselves.

Properties of homomorphisms

Now, we see some properties of homomorphisms themselves.

- Given any group G, the identity function $\mathrm{id}_G : G \to G$ is a homomorphism from G to itself.

Properties of homomorphisms

Now, we see some properties of homomorphisms themselves.

- Given any group G, the identity function $\mathrm{id}_G : G \to G$ is a homomorphism from G to itself.
- Given homomorphisms

$$G \xrightarrow{\varphi} H \xrightarrow{\psi} K,$$

  the composition $\psi \circ \varphi$ is a function from G to K. Moreover, it is a homomorphism.

Properties of homomorphisms

Now, we see some properties of homomorphisms themselves.

- Given any group G, the identity function $\mathrm{id}_G : G \to G$ is a homomorphism from G to itself.
- Given homomorphisms

  $$G \xrightarrow{\varphi} H \xrightarrow{\psi} K,$$

  the composition $\psi \circ \varphi$ is a function from G to K. Moreover, it is a homomorphism.
  Said simply: composition of homomorphisms is again a homomorphism.

Properties of homomorphisms

Now, we see some properties of homomorphisms themselves.

- Given any group G, the identity function $\mathrm{id}_G : G \to G$ is a homomorphism from G to itself.
- Given homomorphisms

$$G \xrightarrow{\varphi} H \xrightarrow{\psi} K,$$

  the composition $\psi \circ \varphi$ is a function from G to K. Moreover, it is a homomorphism.
  Said simply: composition of homomorphisms is again a homomorphism.
- With the same notation as above, we always have

$$\mathrm{id}_H \circ \varphi = \varphi, \quad \psi \circ \mathrm{id}_H = \psi.$$

Properties of homomorphisms

Now, we see some properties of homomorphisms themselves.

- Given any group G, the identity function $\text{id}_G : G \to G$ is a homomorphism from G to itself.
- Given homomorphisms

$$G \xrightarrow{\varphi} H \xrightarrow{\psi} K,$$

  the composition $\psi \circ \varphi$ is a function from G to K. Moreover, it is a homomorphism.
  Said simply: composition of homomorphisms is again a homomorphism.
- With the same notation as above, we always have

$$\text{id}_H \circ \varphi = \varphi, \quad \psi \circ \text{id}_H = \psi.$$

Go look up what a Category is.

Properties of homomorphisms

Now, we see some properties of homomorphisms themselves.

- Given any group G, the identity function $\text{id}_G : G \to G$ is a homomorphism from G to itself.
- Given homomorphisms

$$G \xrightarrow{\varphi} H \xrightarrow{\psi} K,$$

  the composition $\psi \circ \varphi$ is a function from G to K. Moreover, it is a homomorphism.
  Said simply: composition of homomorphisms is again a homomorphism.
- With the same notation as above, we always have

$$\text{id}_H \circ \varphi = \varphi, \quad \psi \circ \text{id}_H = \psi.$$

Go look up what a Category is. (In the context of Category Theory.)

Examples

Let $\mathbb{R}^\times$ denote the group of nonzero real numbers under $\cdot$. Similarly, we have $\mathbb{Q}^\times$ and $\mathbb{C}^\times$.

Examples

Let $\mathbb{R}^\times$ denote the group of nonzero real numbers under $\cdot$. Similarly, we have $\mathbb{Q}^\times$ and $\mathbb{C}^\times$.

- The map $\exp : \mathbb{R} \to \mathbb{R}^\times$ defined by

$$\exp(x) = e^x$$

  is a homomorphism because

$$\exp(x + y) = e^x \cdot e^y = \exp(x) \cdot \exp(y).$$

Examples

Let $\mathbb{R}^\times$ denote the group of nonzero real numbers under $\cdot$. Similarly, we have $\mathbb{Q}^\times$ and $\mathbb{C}^\times$.

- The map $\exp : \mathbb{R} \to \mathbb{R}^\times$ defined by

$$\exp(x) = e^x$$

is a homomorphism because

$$\exp(x + y) = e^x \cdot e^y = \exp(x) \cdot \exp(y).$$

- In the same way, the map $\exp : \mathbb{C} \to \mathbb{C}^\times$ is a group homomorphism.

Examples

Let $\mathbb{R}^\times$ denote the group of nonzero real numbers under $\cdot$. Similarly, we have $\mathbb{Q}^\times$ and $\mathbb{C}^\times$.

- The map $\exp : \mathbb{R} \to \mathbb{R}^\times$ defined by
$$\exp(x) = e^x$$
is a homomorphism because
$$\exp(x + y) = e^x \cdot e^y = \exp(x) \cdot \exp(y).$$

- In the same way, the map $\exp : \mathbb{C} \to \mathbb{C}^\times$ is a group homomorphism. In fact, this is surjective.

Examples

Let $\mathbb{R}^\times$ denote the group of nonzero real numbers under $\cdot$. Similarly, we have $\mathbb{Q}^\times$ and $\mathbb{C}^\times$.

- The map $\exp : \mathbb{R} \to \mathbb{R}^\times$ defined by

$$\exp(x) = e^x$$

  is a homomorphism because

$$\exp(x + y) = e^x \cdot e^y = \exp(x) \cdot \exp(y).$$

- In the same way, the map $\exp : \mathbb{C} \to \mathbb{C}^\times$ is a group homomorphism. In fact, this is surjective.
- Given any $n \in \mathbb{Z}$, the map $\varphi : \mathbb{Z} \to \mathbb{Z}$ defined as

$$\varphi(z) = nz$$

  is a homomorphism.

Examples

Let $\mathbb{R}^\times$ denote the group of nonzero real numbers under $\cdot$. Similarly, we have $\mathbb{Q}^\times$ and $\mathbb{C}^\times$.

- The map $\exp : \mathbb{R} \to \mathbb{R}^\times$ defined by

$$\exp(x) = e^x$$

  is a homomorphism because

$$\exp(x + y) = e^x \cdot e^y = \exp(x) \cdot \exp(y).$$

- In the same way, the map $\exp : \mathbb{C} \to \mathbb{C}^\times$ is a group homomorphism. In fact, this is surjective.
- Given any $n \in \mathbb{Z}$, the map $\varphi : \mathbb{Z} \to \mathbb{Z}$ defined as

$$\varphi(z) = nz$$

  is a homomorphism.
- In general, if G is an abelian group and $n \in \mathbb{Z}$, the map $x \mapsto x^n$ is a homomorphism.

Isomorphisms

Homomorphisms lead to another equally recurring concept in mathematics.

Isomorphisms

Homomorphisms lead to another equally recurring concept in mathematics. The concept of isomorphism.

Isomorphisms

Homomorphisms lead to another equally recurring concept in mathematics. The concept of isomorphism. Loosely speaking, an isomorphism captures two structures to be "equivalent."

Isomorphisms

Homomorphisms lead to another equally recurring concept in mathematics. The concept of isomorphism. Loosely speaking, an isomorphism captures two structures to be "equivalent."

For example, consider the group $\{0, 1, 2\}$ with addition modulo 3 and the group $\{1, \omega, \omega^2\}$ with multiplication. ($\omega = \exp\left(\frac{2\pi}{3}i\right)$.)

Isomorphisms

Homomorphisms lead to another equally recurring concept in mathematics. The concept of isomorphism. Loosely speaking, an isomorphism captures two structures to be "equivalent."

For example, consider the group $\{0, 1, 2\}$ with addition modulo 3 and the group $\{1, \omega, \omega^2\}$ with multiplication. ($\omega = \exp\left(\frac{2\pi}{3} i\right)$.)

While the groups are not equal (since they don't have the same element), they pretty much are same in terms of the group properties.

Isomorphisms

Homomorphisms lead to another equally recurring concept in mathematics. The concept of isomorphism. Loosely speaking, an isomorphism captures two structures to be "equivalent."

For example, consider the group $\{0, 1, 2\}$ with addition modulo 3 and the group $\{1, \omega, \omega^2\}$ with multiplication. ($\omega = \exp\left(\frac{2\pi}{3}i\right)$.)

While the groups are not equal (since they don't have the same element), they pretty much are same in terms of the group properties.
This idea can formalised as follows.

Isomorphisms

Definition 9 (Isomorphism)

Let G and H be groups. A group homomorphism $\varphi : G \to H$ is said to be an *isomorphism* if φ is bijective.

Isomorphisms

Definition 9 (Isomorphism)

Let G and H be groups. A group homomorphism $\varphi : G \to H$ is said to be an *isomorphism* if φ is bijective.

Remark. It can be checked that the inverse of a bijective homomorphism is again a homomorphism.

Isomorphisms

Definition 9 (Isomorphism)

Let G and H be groups. A group homomorphism $\varphi : G \to H$ is said to be an *isomorphism* if φ is bijective.

Remark. It can be checked that the inverse of a bijective homomorphism is again a homomorphism. In particular, if φ is an isomorphism, then so is φ^{-1}.

Isomorphisms

Definition 9 (Isomorphism)

Let G and H be groups. A group homomorphism $\varphi : G \to H$ is said to be an *isomorphism* if φ is bijective.

Remark. It can be checked that the inverse of a bijective homomorphism is again a homomorphism. In particular, if φ is an isomorphism, then so is φ^{-1}.

Definition 10 (Isomorphic)

Two groups G and H are said to be isomorphic if there exists a group isomorphism $\varphi : G \to H$.
In such a case, we write $G \cong H$.

Isomorphisms

Definition 9 (Isomorphism)

Let G and H be groups. A group homomorphism $\varphi : G \to H$ is said to be an *isomorphism* if φ is bijective.

Remark. It can be checked that the inverse of a bijective homomorphism is again a homomorphism. In particular, if φ is an isomorphism, then so is φ^{-1}.

Definition 10 (Isomorphic)

Two groups G and H are said to be isomorphic if there exists a group isomorphism $\varphi : G \to H$.
In such a case, we write $G \cong H$.

One can note that $\cong$ is an "equivalence relation".

Examples

Examples

- With $G = \{0, 1, 2\}$ and $H = \{1, \omega, \omega^2\}$ as earlier, we see that $\varphi : G \to H$ defined by $\varphi(i) = \omega^i$ is an isomorphism.

Examples

- With $G = \{0, 1, 2\}$ and $H = \{1, \omega, \omega^2\}$ as earlier, we see that $\varphi : G \to H$ defined by $\varphi(i) = \omega^i$ is an isomorphism.
- In general, the groups $G = \{0, \ldots, n-1\}$ and $H = \{z \in \mathbb{C}^\times : z^n = 1\}$ are isomorphic.

Examples

- With $G = \{0, 1, 2\}$ and $H = \{1, \omega, \omega^2\}$ as earlier, we see that $\varphi : G \to H$ defined by $\varphi(i) = \omega^i$ is an isomorphism.
- In general, the groups $G = \{0, \ldots, n-1\}$ and $H = \{z \in \mathbb{C}^\times : z^n = 1\}$ are isomorphic.
- The map $\exp : \mathbb{R} \to \mathbb{R}^+$ is an isomorphism. (Note that $\mathbb{R}$ is a group under $+$ whereas $\mathbb{R}^+$ is a group under $\cdot$.)

Kernels

Once again, let us look at a concept the quite recurring in mathematics. (This time more focused in the realm of algebra.)

Kernels

Once again, let us look at a concept the quite recurring in mathematics. (This time more focused in the realm of algebra.)

Definition 11 (Kernel)

Given a group homomorphism $\varphi : G \to H$, we denote the *kernel* of φ by $\ker \varphi$ and define it as

$$\ker \varphi := \{g \in G : \varphi(g) = e_H\}.$$

Kernels

Once again, let us look at a concept the quite recurring in mathematics. (This time more focused in the realm of algebra.)

Definition 11 (Kernel)

Given a group homomorphism $\varphi : G \to H$, we denote the *kernel* of φ by $\ker \varphi$ and define it as

$$\ker \varphi := \{g \in G : \varphi(g) = e_H\}.$$

That is, it is the subset of G consisting of all those elements that get mapped to the identity of H.

Kernels

Once again, let us look at a concept the quite recurring in mathematics. (This time more focused in the realm of algebra.)

Definition 11 (Kernel)

Given a group homomorphism $\varphi : G \to H$, we denote the *kernel* of φ by $\ker \varphi$ and define it as

$$\ker \varphi := \{g \in G : \varphi(g) = e_H\}.$$

That is, it is the subset of G consisting of all those elements that get mapped to the identity of H. Does this remind you of anything from linear algebra?

Kernels

Once again, let us look at a concept the quite recurring in mathematics. (This time more focused in the realm of algebra.)

Definition 11 (Kernel)

Given a group homomorphism $\varphi : G \to H$, we denote the *kernel* of φ by $\ker \varphi$ and define it as

$$\ker \varphi := \{g \in G : \varphi(g) = e_H\}.$$

That is, it is the subset of G consisting of all those elements that get mapped to the identity of H. Does this remind you of anything from linear algebra?

Proposition 5

With the same notations as above, we have

$$\ker \varphi \leq G.$$

A curious property about kernels

Proposition 6

Let $\varphi : G \to H$ and $K = \ker \varphi$.
Then, given any $a \in G$ and $k \in K$, we have

$$aka^{-1} \in K.$$

A curious property about kernels

Proposition 6

Let $\varphi : G \to H$ and $K = \ker \varphi$.
Then, given any $a \in G$ and $k \in K$, we have

$$aka^{-1} \in K.$$

The above says that $aKa^{-1} \subset K$

A curious property about kernels

Proposition 6

Let $\varphi : G \to H$ and $K = \ker \varphi$.
Then, given any $a \in G$ and $k \in K$, we have

$$aka^{-1} \in K.$$

The above says that $aKa^{-1} \subset K$, where aKa^{-1} is defined in the natural manner as

$$\{aka^{-1} : k \in K\}.$$

A curious property about kernels

Proposition 6

Let $\varphi : G \to H$ and $K = \ker \varphi$.
Then, given any $a \in G$ and $k \in K$, we have

$$aka^{-1} \in K.$$

The above says that $aKa^{-1} \subset K$, where aKa^{-1} is defined in the natural manner as

$$\{aka^{-1} : k \in K\}.$$

In fact, since the above is true for all $a \in G$, it is also true for a^{-1} and we actually get the equality $aKa^{-1} = K$.

A curious property about kernels

Proposition 6

Let $\varphi : G \to H$ and $K = \ker \varphi$.
Then, given any $a \in G$ and $k \in K$, we have

$$aka^{-1} \in K.$$

The above says that $aKa^{-1} \subset K$, where aKa^{-1} is defined in the natural manner as

$$\{aka^{-1} : k \in K\}.$$

In fact, since the above is true for all $a \in G$, it is also true for a^{-1} and we actually get the equality $aKa^{-1} = K$.

This can be written in yet another way as $aK = Ka$.

A curious calculation

Now, suppose that $a, a', b, b' \in G$ are elements such that $aK = a'K$ and $bK = b'K$.

A curious calculation

Now, suppose that $a, a', b, b' \in G$ are elements such that $aK = a'K$ and $bK = b'K$.
Then, we see that

A curious calculation

Now, suppose that $a, a', b, b' \in G$ are elements such that $aK = a'K$ and $bK = b'K$.
Then, we see that

$$(ab)K = a(bK)$$

A curious calculation

Now, suppose that $a, a', b, b' \in G$ are elements such that $aK = a'K$ and $bK = b'K$.
Then, we see that

$$\begin{aligned}(ab)K &= a(bK) \\ &= a(Kb)\end{aligned}$$

A curious calculation

Now, suppose that $a, a', b, b' \in G$ are elements such that $aK = a'K$ and $bK = b'K$.
Then, we see that

$$\begin{aligned}(ab)K &= a(bK)\\ &= a(Kb)\\ &= a(Kb')\end{aligned}$$

A curious calculation

Now, suppose that $a, a', b, b' \in G$ are elements such that $aK = a'K$ and $bK = b'K$.
Then, we see that

$$\begin{aligned}(ab)K &= a(bK)\\ &= a(Kb)\\ &= a(Kb')\\ &= (aK)b'\end{aligned}$$

A curious calculation

Now, suppose that $a, a', b, b' \in G$ are elements such that $aK = a'K$ and $bK = b'K$.
Then, we see that

$$\begin{aligned}(ab)K &= a(bK) \\ &= a(Kb) \\ &= a(Kb') \\ &= (aK)b' \\ &= (a'K)b'\end{aligned}$$

A curious calculation

Now, suppose that $a, a', b, b' \in G$ are elements such that $aK = a'K$ and $bK = b'K$.
Then, we see that

$$\begin{aligned}(ab)K &= a(bK)\\ &= a(Kb)\\ &= a(Kb')\\ &= (aK)b'\\ &= (a'K)b'\\ &= a'(Kb')\end{aligned}$$

A curious calculation

Now, suppose that $a, a', b, b' \in G$ are elements such that $aK = a'K$ and $bK = b'K$.
Then, we see that

$$\begin{aligned}(ab)K &= a(bK)\\ &= a(Kb)\\ &= a(Kb')\\ &= (aK)b'\\ &= (a'K)b'\\ &= a'(Kb')\\ &= (a'b')K.\end{aligned}$$

A curious calculation

Now, suppose that $a, a', b, b' \in G$ are elements such that $aK = a'K$ and $bK = b'K$.
Then, we see that

$$\begin{aligned}(ab)K &= a(bK)\\ &= a(Kb)\\ &= a(Kb')\\ &= (aK)b'\\ &= (a'K)b'\\ &= a'(Kb')\\ &= (a'b')K.\end{aligned}$$

Let us keep this in mind for now. We shall come back to it later.

A curious calculation

Now, suppose that $a, a', b, b' \in G$ are elements such that $aK = a'K$ and $bK = b'K$.
Then, we see that

$$\begin{aligned}(ab)K &= a(bK) \\ &= a(Kb) \\ &= a(Kb') \\ &= (aK)b' \\ &= (a'K)b' \\ &= a'(Kb') \\ &= (a'b')K.\end{aligned}$$

Let us keep this in mind for now. We shall come back to it later. Note that the only property we used was that $gK = Kg$ and not really that K was a kernel.

Coming back to cosets

Recall the set of cosets G/H.

Coming back to cosets

Recall the set of cosets G/H. We wish to turn this set into a group.

Coming back to cosets

Recall the set of cosets G/H. We wish to turn this set into a group.

What should the group operation be?

Coming back to cosets

Recall the set of cosets G/H. We wish to turn this set into a group.

What should the group operation be?
Well, given cosets aH and bH, we wish to define $(aH)(bH)$.

Coming back to cosets

Recall the set of cosets G/H. We wish to turn this set into a group.

What should the group operation be?
Well, given cosets aH and bH, we wish to define $(aH)(bH)$.
Moreover, the product must again be a coset.

Coming back to cosets

Recall the set of cosets G/H. We wish to turn this set into a group.

What should the group operation be?
Well, given cosets aH and bH, we wish to define $(aH)(bH)$.
Moreover, the product must again be a coset.

So, the question is: What $g \in G$ should be pick to define

$$(aH)(bH) = gH?$$

Coming back to cosets

Recall the set of cosets G/H. We wish to turn this set into a group.

What should the group operation be?
Well, given cosets aH and bH, we wish to define $(aH)(bH)$.
Moreover, the product must again be a coset.

So, the question is: What $g \in G$ should be pick to define

$$(aH)(bH) = gH?$$

Well, the natural choice is: $g = ab$.

Coming back to cosets

Recall the set of cosets G/H. We wish to turn this set into a group.

What should the group operation be?
Well, given cosets aH and bH, we wish to define $(aH)(bH)$.
Moreover, the product must again be a coset.

So, the question is: What $g \in G$ should be pick to define

$$(aH)(bH) = gH?$$

Well, the natural choice is: $g = ab$.
However, there is a problem...

A problem :(

When we talk about the product $(aH)(bH)$, we are defining products of two *sets*.

A problem :(

When we talk about the product $(aH)(bH)$, we are defining products of two *sets*.
Now, given any coset of H, it is true that it can be written as aH for *some* $a \in G$.

A problem :(

When we talk about the product $(aH)(bH)$, we are defining products of two *sets*.
Now, given any coset of H, it is true that it can be written as aH for *some* $a \in G$.
However, the problem is that the a is not (always) unique.

A problem :(

When we talk about the product $(aH)(bH)$, we are defining products of two *sets*.
Now, given any coset of H, it is true that it can be written as aH for *some* $a \in G$.
However, the problem is that the a is not (always) unique.
Thus, when defining the product, the product must not depend on the representative chosen.

A problem :(

When we talk about the product $(aH)(bH)$, we are defining products of two *sets*.
Now, given any coset of H, it is true that it can be written as aH for *some* $a \in G$.
However, the problem is that the a is not (always) unique.
Thus, when defining the product, the product must not depend on the representative chosen.
This means that we must take care of the following:

A problem :(

When we talk about the product $(aH)(bH)$, we are defining products of two *sets*.
Now, given any coset of H, it is true that it can be written as aH for *some* $a \in G$.
However, the problem is that the a is not (always) unique.
Thus, when defining the product, the product must not depend on the representative chosen.
This means that we must take care of the following:

Whenever we have $aH = a'H$ and $bH = b'H$

A problem :(

When we talk about the product $(aH)(bH)$, we are defining products of two *sets*.

Now, given any coset of H, it is true that it can be written as aH for *some* $a \in G$.

However, the problem is that the a is not (always) unique.

Thus, when defining the product, the product must not depend on the representative chosen.

This means that we must take care of the following:

Whenever we have $aH = a'H$ and $bH = b'H$, we must have

$$(aH)(bH) = (a'H)(b'H).$$

A problem :(

When we talk about the product $(aH)(bH)$, we are defining products of two *sets*.
Now, given any coset of H, it is true that it can be written as aH for *some* $a \in G$.
However, the problem is that the a is not (always) unique.
Thus, when defining the product, the product must not depend on the representative chosen.
This means that we must take care of the following:

Whenever we have $aH = a'H$ and $bH = b'H$, we must have

$$(aH)(bH) = (ab)H = (a'b')H = (a'H)(b'H).$$

A problem :(

When we talk about the product $(aH)(bH)$, we are defining products of two *sets*.
Now, given any coset of H, it is true that it can be written as aH for *some* $a \in G$.
However, the problem is that the a is not (always) unique.
Thus, when defining the product, the product must not depend on the representative chosen.
This means that we must take care of the following:

Whenever we have $aH = a'H$ and $bH = b'H$, we must have

$$(ab)H = (a'b')H.$$

Solving the problem :)

Well, what does that remind us of?

Solving the problem :)

Well, what does that remind us of? That was a property kernels of homomorphisms have!

Solving the problem :)

Well, what does that remind us of? That was a property kernels of homomorphisms have!
In fact, what we saw was that all we need is that $gH = Hg$ (for all $g \in G$) and then, we always have the desired property.

Solving the problem :)

Well, what does that remind us of? That was a property kernels of homomorphisms have!
In fact, what we saw was that all we need is that $gH = Hg$ (for all $g \in G$) and then, we always have the desired property.

Note that we have shown that if $gH = Hg$, then the multiplication is well-defined.

Solving the problem :)

Well, what does that remind us of? That was a property kernels of homomorphisms have!
In fact, what we saw was that all we need is that $gH = Hg$ (for all $g \in G$) and then, we always have the desired property.

Note that we have shown that if $gH = Hg$, then the multiplication is well-defined.
In fact, the converse is true as well.

Solving the problem :)

Well, what does that remind us of? That was a property kernels of homomorphisms have!
In fact, what we saw was that all we need is that $gH = Hg$ (for all $g \in G$) and then, we always have the desired property.

Note that we have shown that if $gH = Hg$, then the multiplication is well-defined.
In fact, the converse is true as well. That is,

Solving the problem :)

Well, what does that remind us of? That was a property kernels of homomorphisms have!
In fact, what we saw was that all we need is that $gH = Hg$ (for all $g \in G$) and then, we always have the desired property.

Note that we have shown that if $gH = Hg$, then the multiplication is well-defined.
In fact, the converse is true as well. That is, if

$$aH = a'H, bH = b'H \implies (ab)H = (a'b')H,$$

Well, what does that remind us of? That was a property kernels of homomorphisms have!
In fact, what we saw was that all we need is that $gH = Hg$ (for all $g \in G$) and then, we always have the desired property.

Note that we have shown that if $gH = Hg$, then the multiplication is well-defined.
In fact, the converse is true as well. That is, if

$$aH = a'H, bH = b'H \implies (ab)H = (a'b')H,$$

then H must satisfy $gH = Hg$.

Normal subgroups

The previous discussion brings us to an important notion - that of a *normal* subgroup.

The previous discussion brings us to an important notion - that of a *normal* subgroup. What do you think is the definition?

Definition 12 (Normal subgroup)

A subgroup N of a group G is said to be *normal* if

Normal subgroups

The previous discussion brings us to an important notion - that of a *normal* subgroup. What do you think is the definition?

Definition 12 (Normal subgroup)

A subgroup N of a group G is said to be *normal* if

$$gN = Ng$$

for all $g \in G$.

Normal subgroups

The previous discussion brings us to an important notion - that of a *normal* subgroup. What do you think is the definition?

Definition 12 (Normal subgroup)

A subgroup N of a group G is said to be *normal* if

$$gN = Ng$$

for all $g \in G$.

Said differently, we must have $gNg^{-1} = N$ for all $g \in G$.

Normal subgroups

The previous discussion brings us to an important notion - that of a *normal* subgroup. What do you think is the definition?

Definition 12 (Normal subgroup)

A subgroup N of a group G is said to be *normal* if

$$gN = Ng$$

for all $g \in G$.

Said differently, we must have $gNg^{-1} = N$ for all $g \in G$.
Said even more differently, given any $n \in N$, and $g \in G$, we must have $gng^{-1} \in N$.

Quotienting

With this, we come to the last theme for today, another very recurring theme in mathematics

Quotienting

With this, we come to the last theme for today, another very recurring theme in mathematics - *quotienting*.

Quotienting

With this, we come to the last theme for today, another very recurring theme in mathematics - *quotienting*.
We first look at the definition and then have discussion about the theme.

Quotienting

With this, we come to the last theme for today, another very recurring theme in mathematics - *quotienting*.

Definition 13 (Quotient group)

Let G be a group and N be a normal subgroup of G.
Then, the set of cosets G/N is a group under the operation defined by

$$(aN)(bN) := (ab)N,$$

which is well-defined in view of our previous discussion.

Quotienting

With this, we come to the last theme for today, another very recurring theme in mathematics - *quotienting*.

Definition 13 (Quotient group)

Let G be a group and N be a normal subgroup of G.
Then, the set of cosets G/N is a group under the operation defined by

$$(aN)(bN) := (ab)N,$$

which is well-defined in view of our previous discussion.

We sometimes use the notation $\bar{g}$ to denote the coset gH. (When H is clear from context.)

Quotienting

With this, we come to the last theme for today, another very recurring theme in mathematics - *quotienting*.

Definition 13 (Quotient group)

Let G be a group and N be a normal subgroup of G.
Then, the set of cosets G/N is a group under the operation defined by

$$(aN)(bN) := (ab)N,$$

which is well-defined in view of our previous discussion.

We sometimes use the notation $\bar{g}$ to denote the coset gH. (When H is clear from context.)
Another thing to note is that any subgroup of an abelian group is normal.

Example

Consider the group $(\mathbb{Z}, +)$ and the subgroup $5\mathbb{Z}$. (Is this normal?)

Example

Consider the group $(\mathbb{Z}, +)$ and the subgroup $5\mathbb{Z}$. (Is this normal?) (Since the group operation is denoted with $+$, we will use $+$ to denote the cosets as well.)

Example

Consider the group $(\mathbb{Z}, +)$ and the subgroup $5\mathbb{Z}$. (Is this normal?) (Since the group operation is denoted with $+$, we will use $+$ to denote the cosets as well.)
As an example, one of the cosets of $5\mathbb{Z}$ is

$$2 + 5\mathbb{Z} = \{\dots, -8, -3, 2, 7, 12, \dots\}.$$

Example

Consider the group $(\mathbb{Z}, +)$ and the subgroup $5\mathbb{Z}$. (Is this normal?) (Since the group operation is denoted with $+$, we will use $+$ to denote the cosets as well.)
As an example, one of the cosets of $5\mathbb{Z}$ is

$$2 + 5\mathbb{Z} = \{\dots, -8, -3, 2, 7, 12, \dots\}.$$

The set of cosets is $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$.

Example

Consider the group $(\mathbb{Z}, +)$ and the subgroup $5\mathbb{Z}$. (Is this normal?) (Since the group operation is denoted with $+$, we will use $+$ to denote the cosets as well.)
As an example, one of the cosets of $5\mathbb{Z}$ is

$$2 + 5\mathbb{Z} = \{\dots, -8, -3, 2, 7, 12, \dots\}.$$

The set of cosets is $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$. The addition (as an example) is like

$$\bar{1} + \bar{2} = \bar{3}, \quad \bar{3} + \bar{4} = \bar{2}, \quad \bar{2} + \bar{3} = \bar{0}.$$

Example

Consider the group $(\mathbb{Z}, +)$ and the subgroup $5\mathbb{Z}$. (Is this normal?) (Since the group operation is denoted with $+$, we will use $+$ to denote the cosets as well.)
As an example, one of the cosets of $5\mathbb{Z}$ is

$$2 + 5\mathbb{Z} = \{\dots, -8, -3, 2, 7, 12, \dots\}.$$

The set of cosets is $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$. The addition (as an example) is like

$$\bar{1} + \bar{2} = \bar{3}, \quad \bar{3} + \bar{4} = \bar{2}, \quad \bar{2} + \bar{3} = \bar{0}.$$

Basically, this is just addition modulo 5.

Example

Consider the group $(\mathbb{Z}, +)$ and the subgroup $5\mathbb{Z}$. (Is this normal?) (Since the group operation is denoted with $+$, we will use $+$ to denote the cosets as well.)
As an example, one of the cosets of $5\mathbb{Z}$ is

$$2 + 5\mathbb{Z} = \{\ldots, -8, -3, 2, 7, 12, \ldots\}.$$

The set of cosets is $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$. The addition (as an example) is like

$$\bar{1} + \bar{2} = \bar{3}, \quad \bar{3} + \bar{4} = \bar{2}, \quad \bar{2} + \bar{3} = \bar{0}.$$

Basically, this is just addition modulo 5.

The above group is what is called $\mathbb{Z}/5\mathbb{Z}$.

Example

Consider the group $(\mathbb{Z}, +)$ and the subgroup $5\mathbb{Z}$. (Is this normal?) (Since the group operation is denoted with $+$, we will use $+$ to denote the cosets as well.)
As an example, one of the cosets of $5\mathbb{Z}$ is

$$2 + 5\mathbb{Z} = \{\dots, -8, -3, 2, 7, 12, \dots\}.$$

The set of cosets is $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$. The addition (as an example) is like

$$\bar{1} + \bar{2} = \bar{3}, \quad \bar{3} + \bar{4} = \bar{2}, \quad \bar{2} + \bar{3} = \bar{0}.$$

Basically, this is just addition modulo 5.

The above group is what is called $\mathbb{Z}/5\mathbb{Z}$. Of course, this works for all values of 5.

Example

Consider the group $(\mathbb{Z}, +)$ and the subgroup $5\mathbb{Z}$. (Is this normal?) (Since the group operation is denoted with $+$, we will use $+$ to denote the cosets as well.)
As an example, one of the cosets of $5\mathbb{Z}$ is

$$2 + 5\mathbb{Z} = \{\dots, -8, -3, 2, 7, 12, \dots\}.$$

The set of cosets is $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$. The addition (as an example) is like

$$\bar{1} + \bar{2} = \bar{3}, \quad \bar{3} + \bar{4} = \bar{2}, \quad \bar{2} + \bar{3} = \bar{0}.$$

Basically, this is just addition modulo 5.

The above group is what is called $\mathbb{Z}/5\mathbb{Z}$. Of course, this works for all values of 5.
In fact, this is the group (up to isomorphism) which we saw earlier as $\{1, \dots, n-1\}$ with addition modulo n.

Exercises

1. Let $(G, \cdot)$ be a finite group and let $x \in G$.
Show that $H = \{1, x, x^2, \ldots\}$ is a (finite) subgroup of G.

Show that H has order $|x|$.

Conclude that $|x|$ divides $|G|$.
In particular, we have $x^{|G|} = e$.

2. Let $n > 1$ be a natural number. Define

$$(\mathbb{Z}/n\mathbb{Z})^* = \{x : 1 \leq x \leq n, \gcd(x, n) = 1\}.$$

Show that $|(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(n)$, where φ is the Euler totient function.

Show that $(\mathbb{Z}/n\mathbb{Z})^*$ is a group under the operation "multiplication mod n" with identity being 1.

Conclude that $a^{\varphi(n)} = 1$ for all $a \in (\mathbb{Z}/n\mathbb{Z})^*$. (Note that this equality is in the group $(\mathbb{Z}/n\mathbb{Z})^*$.)

Conclude that $a^{\varphi(n)} \equiv 1 \bmod n$ for all a with $\gcd(a, n) = 1$.

This is Euler's theorem (in number theory) and Fermat's little theorem is a special case of it.

3. Let G be a finite group and let p be a prime dividing $|G|$. Let $\mathcal{S}$ denote the set of p-tuples of elements of G the product of whose coordinates is 1 :

$$\mathcal{S} = \{(x_1, \ldots, x_p) : x_i \in G \text{ and } x_1 x_2 \cdots x_p = 1\}.$$

(a) Show that $\mathcal{S}$ has $|G|^{p-1}$ elements, hence has order divisible by p.

Define the relation $\sim$ on $\mathcal{S}$ be letting $\alpha \sim \beta$ if β is a cyclic permutation of α.

(b) Show that a cyclic permutation of an element of $\mathcal{S}$ is again an element of $\mathcal{S}$.
(c) Prove that $\sim$ is an equivalence relation on $\mathcal{S}$.
(d) Prove that an equivalence class contains a single element if and only if it is of the form $(x, \ldots, x)$ with $x^p = 1$.

(e) Prove that every equivalence class has order 1 or p (this uses the fact that p is a *prime*). Deduce that $|G|^{p-1} = k + pd$ where k is the number of classes of size 1 and d is the number of classes of size p.
(f) Since $\{(1, \ldots, 1)\}$ is an equivalence class of size 1, conclude from (e) that there must be a nonidentity element x in G with $x^p = 1$, i.e., G contains an element of order P. (Show $p \mid k$ and so $k > 1$.)

The previous exercise proves the following theorem.

Theorem 2 (Cauchy's Theorem)

If G is a finite group and $p \mid |G|$, then there exists $x \in G$ such that $p = |x|$.

With $H = \{1, x, \ldots\}$ as in Exercise 1, this shows that there exists a subgroup of order p.
This is a partial converse to Lagrange's theorem (and the statement shown in Exercise 1).
(And that's the best we can get.)

Credits: The above style of proof was published in Amer. Math. Monthly, 66 (1959), p. 199 by James McKay.
The above exercise has been taken from Abstract Algebra by Dummit and Foote.

4. Let $n \geq 1$ be a natural number and define

$$[n] = \{1, \ldots, n\}.$$

Let S_n denote the set of all *bijections* from $[n]$ to $[n]$.
Let $\circ$ denote the usual composition operation of functions.

(a) Show that $\circ$ is a binary operation on S_n.
(b) Show that S_n is a group under $\circ$.
This is known as the *symmetric group* on n elements.
This is a very common example of a (family of) group.
(c) Show that S_n is abelian if and only if $n \leq 2$.

A remarkable theorem called *Cayley's theorem* says that any (finite) group is isomorphic to a subgroup of S_n for some n.