WELCOME

Group Theory

J. Maria Joseph Ph.D.,

Assistant Professor, Department of Mathematics,
St. Joseph's College, Trichy - 2.

July 1, 2015

Outline

Towers of Hanoi

Towers of Hanoi

Hello Friends, are you willing to destroy this world ?

Towers of Hanoi

Hello Friends, are you willing to destroy this world ?
It's very easy.

Towers of Hanoi

Hello Friends, are you willing to destroy this world ?
It's very easy. Just you have to solve one problem.

Towers of Hanoi

Hello Friends, are you willing to destroy this world ?
It's very easy. Just you have to solve one problem.
Are you ready ?

Towers of Hanoi

Hello Friends, are you willing to destroy this world ?
It's very easy. Just you have to solve one problem.
Are you ready ? Shall we see the problem.

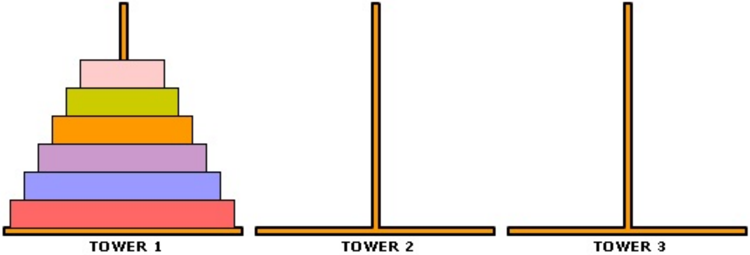
There is a story about an Indian temple in Kashi Vishwanath.

There is a story about an Indian temple in Kashi Vishwanath. The Tower of Hanoi (also called the Tower of Brahma or Lucas' Tower) is a mathematical game or puzzle.

There is a story about an Indian temple in Kashi Vishwanath. The Tower of Hanoi (also called the Tower of Brahma or Lucas' Tower) is a mathematical game or puzzle. It consists of three rods, and a number of disks of different sizes which can slide onto any rod.

There is a story about an Indian temple in Kashi Vishwanath. The Tower of Hanoi (also called the Tower of Brahma or Lucas' Tower) is a mathematical game or puzzle. It consists of three rods, and a number of disks of different sizes which can slide onto any rod. The puzzle starts with the disks in a neat stack in ascending order of size on one rod, the smallest at the top, thus making a conical shape.

Diagram of Hanoi



The objective of the puzzle is to move the entire stack to another rod, obeying the following simple rules:

The objective of the puzzle is to move the entire stack to another rod, obeying the following simple rules:

1. Only one disk can be moved at a time.

The objective of the puzzle is to move the entire stack to another rod, obeying the following simple rules:

1. Only one disk can be moved at a time.
2. Each move consists of taking the upper disk from one of the stacks and placing it on top of another stack i.e. a disk can only be moved if it is the uppermost disk on a stack.

The objective of the puzzle is to move the entire stack to another rod, obeying the following simple rules:

1. Only one disk can be moved at a time.
2. Each move consists of taking the upper disk from one of the stacks and placing it on top of another stack i.e. a disk can only be moved if it is the uppermost disk on a stack.
3. No disk may be placed on top of a smaller disk.

Solution

If the legend were true, and if the priests were able to move disks at a rate of one per second,

Solution

If the legend were true, and if the priests were able to move disks at a rate of one per second, using the smallest number of moves, it would take them $2^{64} - 1$ seconds

Solution

If the legend were true, and if the priests were able to move disks at a rate of one per second, using the smallest number of moves, it would take them $2^{64} - 1$ seconds or roughly 585 billion years

Solution

If the legend were true, and if the priests were able to move disks at a rate of one per second, using the smallest number of moves, it would take them $2^{64} - 1$ seconds or roughly 585 billion years or 18,446,744,073,709,551,615 turns to finish,

Solution

If the legend were true, and if the priests were able to move disks at a rate of one per second, using the smallest number of moves, it would take them $2^{64} - 1$ seconds or roughly 585 billion years or 18,446,744,073,709,551,615 turns to finish, or about 127 times the current age of the sun.

Group Theory

Set

A set is a collection of well-defined objects. The objects of a set are called elements or members of the set.

Set

A set is a collection of well-defined objects. The objects of a set are called elements or members of the set.

Example

(1) The collection of male students in your class.

Set

A set is a collection of well-defined objects. The objects of a set are called elements or members of the set.

Example

(1) The collection of male students in your class.

(2) The collection of numbers 2, 4, 6, 10 and 12.

Set

A set is a collection of well-defined objects. The objects of a set are called elements or members of the set.

Example

(1) The collection of male students in your class.
(2) The collection of numbers 2, 4, 6, 10 and 12.
(3) The collection of districts in Tamil Nadu.

Operation

Now that we have elements of sets it would be nice to do things with them.

Operation

Now that we have elements of sets it would be nice to do things with them. Specifically, we wish to combine them in some way.

Operation

Now that we have elements of sets it would be nice to do things with them. Specifically, we wish to combine them in some way. This is what an operation is used for.

Operation

Now that we have elements of sets it would be nice to do things with them. Specifically, we wish to combine them in some way. This is what an operation is used for.

An operation takes elements of a set,

Operation

Now that we have elements of sets it would be nice to do things with them. Specifically, we wish to combine them in some way. This is what an operation is used for.

An operation takes elements of a set, combines them in some way,

Operation

Now that we have elements of sets it would be nice to do things with them. Specifically, we wish to combine them in some way. This is what an operation is used for.

An operation takes elements of a set, combines them in some way, and produces another element.

Operation

Now that we have elements of sets it would be nice to do things with them. Specifically, we wish to combine them in some way. This is what an operation is used for.

An operation takes elements of a set, combines them in some way, and produces another element.

An operation combines members of a set.

I can use painting as an Example

Let's imagine we have the set of colors { red, green, blue }.

I can use painting as an Example

Let's imagine we have the set of colors { red, green, blue }. Now we have to define an operation, and one that makes the most sense is mixing.

I can use painting as an Example

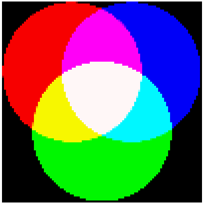
Let's imagine we have the set of colors { red, green, blue }. Now we have to define an operation, and one that makes the most sense is mixing. So for example, red mixed with green makes yellow,

I can use painting as an Example

Let's imagine we have the set of colors { red, green, blue }. Now we have to define an operation, and one that makes the most sense is mixing. So for example, red mixed with green makes yellow, and red mixed with blue makes purple.

I can use painting as an Example

Let's imagine we have the set of colors { red, green, blue }. Now we have to define an operation, and one that makes the most sense is mixing. So for example, red mixed with green makes yellow, and red mixed with blue makes purple.



Binary Operations

So far we have been a little bit too general.

Binary Operations

So far we have been a little bit too general. So we will now be a little bit more specific.

Binary Operations

So far we have been a little bit too general. So we will now be a little bit more specific. A binary operation is just like an operation,

Binary Operations

So far we have been a little bit too general. So we will now be a little bit more specific. A binary operation is just like an operation, except that it takes 2 elements, no more, no less, and combines them into one.

Binary Operations

So far we have been a little bit too general. So we will now be a little bit more specific. A binary operation is just like an operation, except that it takes 2 elements, no more, no less, and combines them into one.

Example

You already know a few binary operators, even though you may not know that you know them:

Binary Operations

So far we have been a little bit too general. So we will now be a little bit more specific. A binary operation is just like an operation, except that it takes 2 elements, no more, no less, and combines them into one.

Example

You already know a few binary operators, even though you may not know that you know them:

- $5 + 3 = 8$

Binary Operations

So far we have been a little bit too general. So we will now be a little bit more specific. A binary operation is just like an operation, except that it takes 2 elements, no more, no less, and combines them into one.

Example

You already know a few binary operators, even though you may not know that you know them:

- $5 + 3 = 8$
- $4 \times 3 = 12$

Binary Operations

So far we have been a little bit too general. So we will now be a little bit more specific. A binary operation is just like an operation, except that it takes 2 elements, no more, no less, and combines them into one.

Example

You already know a few binary operators, even though you may not know that you know them:

- $5 + 3 = 8$
- $4 \times 3 = 12$
- $4 - 4 = 0$

Formal Definition

Let S be a non - empty set.

Formal Definition

Let S be a non - empty set. $*$ is a binary operation defined on S is function

$$* : S \times S \to S \text{ by } (a, b) \to a * b$$

Formal Definition

Let S be a non - empty set. $*$ is a binary operation defined on S is function

$$* : S \times S \to S \text{ by } (a, b) \to a * b$$

That is

$$a, b \in S \Longrightarrow a * b \in S$$

Introduction to Groups

Now that we understand sets and operators, you know the basic building blocks that make up groups. Simply put

Introduction to Groups

Now that we understand sets and operators, you know the basic building blocks that make up groups. Simply put

A group is a set combined with an operation

Group

A group is a set G, combined with an operation $*$, such that

Group

A group is a set G, combined with an operation $*$, such that

❋ The group is closed under the operation

Group

A group is a set G, combined with an operation $*$, such that

- The group is closed under the operation
- The operation is associative

Group

A group is a set G, combined with an operation $*$, such that

- ❋ The group is closed under the operation
- ❋ The operation is associative
- ❋ The group contains an identity

Group

A group is a set G, combined with an operation $*$, such that

- ❋ The group is closed under the operation
- ❋ The operation is associative
- ❋ The group contains an identity
- ❋ The group contains inverse

Closed under the operation

Imagine you are closed inside a huge box.

Closed under the operation

Imagine you are closed inside a huge box. When you are on the inside, you can't get to the outside.

Closed under the operation

Imagine you are closed inside a huge box. When you are on the inside, you can't get to the outside. In that same way, once you have two elements inside the group, no matter what the elements are,

Closed under the operation

Imagine you are closed inside a huge box. When you are on the inside, you can't get to the outside. In that same way, once you have two elements inside the group, no matter what the elements are, using the operation on them will not get you outside the group

Closed under the operation

Imagine you are closed inside a huge box. When you are on the inside, you can't get to the outside. In that same way, once you have two elements inside the group, no matter what the elements are, using the operation on them will not get you outside the group

If we have two elements in the group, a and b,

Closed under the operation

Imagine you are closed inside a huge box. When you are on the inside, you can't get to the outside. In that same way, once you have two elements inside the group, no matter what the elements are, using the operation on them will not get you outside the group

If we have two elements in the group, a and b, it must be the case that $a * b$ is also in the group.

Closed under the operation

Imagine you are closed inside a huge box. When you are on the inside, you can't get to the outside. In that same way, once you have two elements inside the group, no matter what the elements are, using the operation on them will not get you outside the group

If we have two elements in the group, a and b, it must be the case that $a * b$ is also in the group. This is what we mean by closed.

Formal Statement

For all elements a, b in G, $a * b$ is in G

Associative

You should have learned about associative way back in basic algebra.

Associative

You should have learned about associative way back in basic algebra. All it means is that the order in which we do operations doesn't matter.

Associative

You should have learned about associative way back in basic algebra. All it means is that the order in which we do operations doesn't matter.

$$a * (b * c) = (a * b) * c$$

Associative

You should have learned about associative way back in basic algebra. All it means is that the order in which we do operations doesn't matter.

$$a * (b * c) = (a * b) * c$$

Formal Statement

For all a, b and c in G, $a * (b * c) = (a * b) * c$

The group contains inverses

If we have an element of the group,

The group contains inverses

If we have an element of the group, there is another element of the group

The group contains inverses

If we have an element of the group, there is another element of the group such that when we use the operator on both of them,

The group contains inverses

If we have an element of the group, there is another element of the group such that when we use the operator on both of them, we get e, the identity.

The group contains inverses

If we have an element of the group, there is another element of the group such that when we use the operator on both of them, we get e, the identity.

Formal Statement

For all a in G, there exists b in G,

The group contains inverses

If we have an element of the group, there is another element of the group such that when we use the operator on both of them, we get e, the identity.

Formal Statement

For all a in G, there exists b in G, such that

$$a * b = e$$

The group contains inverses

If we have an element of the group, there is another element of the group such that when we use the operator on both of them, we get e, the identity.

Formal Statement

For all a in G, there exists b in G, such that
$a * b = e$ and $b * a = e$.

The group contains an identity

If we use the operation on any element and the identity, we will get that element back.

The group contains an identity

If we use the operation on any element and the identity, we will get that element back.

Formal Statement

There exists an e in the set G,

The group contains an identity

If we use the operation on any element and the identity, we will get that element back.

Formal Statement

There exists an e in the set G, such that $a * e = a$

The group contains an identity

If we use the operation on any element and the identity, we will get that element back.

Formal Statement

There exists an e in the set G, such that $a * e = a$ and $e * a = a$,

The group contains an identity

If we use the operation on any element and the identity, we will get that element back.

Formal Statement

There exists an e in the set G, such that $a * e = a$ and $e * a = a$, for all elements a in G

Formal Definition

A non-empty set G,

Formal Definition

A non-empty set G, together with an operation $*$

Formal Definition

A non-empty set G, together with an operation $*$ i.e., $(G, *)$ is said to be a group if it satisfies the following axioms

- Closure axiom :

Formal Definition

A non-empty set G, together with an operation $*$ i.e., $(G, *)$ is said to be a group if it satisfies the following axioms

- Closure axiom : $a, b \in G \Rightarrow a * b \in G$

Formal Definition

A non-empty set G, together with an operation $*$ i.e., $(G, *)$ is said to be a group if it satisfies the following axioms

- Closure axiom : $a, b \in G \Rightarrow a * b \in G$
- Associative axiom :

Formal Definition

A non-empty set G, together with an operation $*$ i.e., $(G, *)$ is said to be a group if it satisfies the following axioms

- Closure axiom : $a, b \in G \Rightarrow a * b \in G$
- Associative axiom :
  $\forall\, a, b, c \in G,\ (a * b) * c = a * (b * c)$

Formal Definition

A non-empty set G, together with an operation $*$ i.e., $(G, *)$ is said to be a group if it satisfies the following axioms

- Closure axiom : $a, b \in G \Rightarrow a * b \in G$
- Associative axiom : $\forall\, a, b, c \in G,\ (a * b) * c = a * (b * c)$
- Identity axiom :

Formal Definition

A non-empty set G, together with an operation $*$ i.e., $(G, *)$ is said to be a group if it satisfies the following axioms

- **Closure axiom** : $a, b \in G \Rightarrow a * b \in G$
- **Associative axiom** : $\forall\, a, b, c \in G,\ (a * b) * c = a * (b * c)$
- **Identity axiom** : There exists an element $e \in G$ such that $a * e = e * a = a,\ \forall\, a \in G$.

Formal Definition

A non-empty set G, together with an operation $*$ i.e., $(G, *)$ is said to be a group if it satisfies the following axioms

- **Closure axiom** : $a, b \in G \Rightarrow a * b \in G$
- **Associative axiom** : $\forall\, a, b, c \in G$, $(a * b) * c = a * (b * c)$
- **Identity axiom** : There exists an element $e \in G$ such that $a * e = e * a = a$, $\forall\, a \in G$.
- **Inverse axiom** :

Formal Definition

A non-empty set G, together with an operation $*$ i.e., $(G, *)$ is said to be a group if it satisfies the following axioms

- Closure axiom : $a, b \in G \Rightarrow a * b \in G$
- Associative axiom : $\forall\, a, b, c \in G,\ (a * b) * c = a * (b * c)$
- Identity axiom : There exists an element $e \in G$ such that $a * e = e * a = a, \forall\, a \in G$.
- Inverse axiom : $\forall\, a \in G$ there exists an element $a^{-1} \in G$ such that $a^{-1} * a = a * a^{-1} = e$.

Commutative property

A binary operation $*$ on a set G is said to be commutative, if

Commutative property

A binary operation $*$ on a set G is said to be commutative, if

$$a * b = b * a \forall a, b \in S$$

Abelian Group

If a group satisfies the commutative property

Abelian Group

If a group satisfies the commutative property then it is called an abelian group or a commutative group,

Abelian Group

If a group satisfies the commutative property then it is called an abelian group or a commutative group, otherwise it is called a non - abelian group.

Order

The order of a group is defined as the number of distinct elements in the underlying set.

Order

The order of a group is defined as the number of distinct elements in the underlying set.

- If the number of elements is finite then the group is called a finite group

Order

The order of a group is defined as the number of distinct elements in the underlying set.

- If the number of elements is finite then the group is called a finite group
- If the number of elements is infinite then the group is called an infinite group.

Order

The order of a group is defined as the number of distinct elements in the underlying set.

- If the number of elements is finite then the group is called a finite group
- If the number of elements is infinite then the group is called an infinite group.

The order of a group G is denoted by $o(G)$.

Examples

Example 1

Show that $(\mathbb{Z}, +)$ is an infinite abelian group.

Example 1

Show that $(\mathbb{Z}, +)$ is an infinite abelian group.

Solution

$(\mathbb{Z}, +)$ is an abelian. 0 is the identity element.
Inverse exists for each element in $\mathbb{Z}$.

Example 2

Show that $(\mathbb{C}, +)$ is an infinite abelian group.

Solution

Let $z_1, z_2 \in \mathbb{C}$.

Solution

Let $z_1, z_2 \in \mathbb{C}$.

(i) Closure : $z_1 + z_2 \in \mathbb{C} \quad \forall\, z_1, z_2 \in \mathbb{C}$

Solution

Let $z_1, z_2 \in \mathbb{C}$.

(i) Closure : $z_1 + z_2 \in \mathbb{C} \quad \forall\, z_1, z_2 \in \mathbb{C}$

(ii) Associative : Let $z_1, z_2, z_3 \in \mathbb{C}$, then
$$z_1 + (z_2 + z_3) = (z_1 + z_2) + z_3$$

Solution

Let $z_1, z_2 \in \mathbb{C}$.

(i) Closure : $z_1 + z_2 \in \mathbb{C} \quad \forall\, z_1, z_2 \in \mathbb{C}$

(ii) Associative : Let $z_1, z_2, z_3 \in \mathbb{C}$, then
$z_1 + (z_2 + z_3) = (z_1 + z_2) + z_3$

(iii) Identity : $0 = 0 + i0 \in \mathbb{C}$

Solution

Let $z_1, z_2 \in \mathbb{C}$.

(i) Closure : $z_1 + z_2 \in \mathbb{C} \quad \forall\, z_1, z_2 \in \mathbb{C}$

(ii) Associative : Let $z_1, z_2, z_3 \in \mathbb{C}$, then
$z_1 + (z_2 + z_3) = (z_1 + z_2) + z_3$

(iii) Identity : $0 = 0 + i0 \in \mathbb{C}$

(iv) Inverse : Let $z_1 \in \mathbb{C}, \exists - z_1 \in \mathbb{C}$ such that
$z_1 + (-z_1) = 0$

Solution

Let $z_1, z_2 \in \mathbb{C}$.

(i) Closure : $z_1 + z_2 \in \mathbb{C} \quad \forall\, z_1, z_2 \in \mathbb{C}$

(ii) Associative : Let $z_1, z_2, z_3 \in \mathbb{C}$, then
$z_1 + (z_2 + z_3) = (z_1 + z_2) + z_3$

(iii) Identity : $0 = 0 + i0 \in \mathbb{C}$

(iv) Inverse : Let $z_1 \in \mathbb{C}, \exists - z_1 \in \mathbb{C}$ such that
$z_1 + (-z_1) = 0$

(v) Commutative : $z_1 + z_2 = z_2 + z_1 \;\forall\, z_1, z_2 \in \mathbb{C}$.

Solution

Let $z_1, z_2 \in \mathbb{C}$.

(i) Closure : $z_1 + z_2 \in \mathbb{C} \quad \forall\, z_1, z_2 \in \mathbb{C}$

(ii) Associative : Let $z_1, z_2, z_3 \in \mathbb{C}$, then
$z_1 + (z_2 + z_3) = (z_1 + z_2) + z_3$

(iii) Identity : $0 = 0 + i0 \in \mathbb{C}$

(iv) Inverse : Let $z_1 \in \mathbb{C}, \exists - z_1 \in \mathbb{C}$ such that
$z_1 + (-z_1) = 0$

(v) Commutative : $z_1 + z_2 = z_2 + z_1 \,\forall\, z_1, z_2 \in \mathbb{C}$.

$\therefore$ $(\mathbb{C}, +)$ is an abelian group.

Example 3

Show that the set of all non-zero complex numbers is an abelian group under the usual multiplication of complex numbers.

Solution

Let $G = \mathbb{C} - \{0\}$

Solution

Let $G = \mathbb{C} - \{0\}$

(i) Closure : $z_1 \cdot z_2 \in \mathbb{C} \quad \forall\, z_1, z_2 \in \mathbb{C}$

Solution

Let $G = \mathbb{C} - \{0\}$

(i) Closure : $z_1 \cdot z_2 \in \mathbb{C} \quad \forall\, z_1, z_2 \in \mathbb{C}$

(ii) Associative : Let $z_1, z_2, z_3 \in \mathbb{C}$, then $z_1 \cdot (z_2 \cdot z_3) = (z_1 \cdot z_2) \cdot z_3$ (Multiplication is always associative)

Solution

Let $G = \mathbb{C} - \{0\}$

(i) Closure : $z_1 \cdot z_2 \in \mathbb{C} \quad \forall\, z_1, z_2 \in \mathbb{C}$

(ii) Associative : Let $z_1, z_2, z_3 \in \mathbb{C}$, then $z_1 \cdot (z_2 \cdot z_3) = (z_1 \cdot z_2) \cdot z_3$ (Multiplication is always associative)

(iii) Identity : $1 = 1 + i0 \in \mathbb{C}$ is the identity element

Solution

Let $G = \mathbb{C} - \{0\}$

(i) Closure : $z_1 \cdot z_2 \in \mathbb{C} \quad \forall\, z_1, z_2 \in \mathbb{C}$

(ii) Associative : Let $z_1, z_2, z_3 \in \mathbb{C}$, then $z_1 \cdot (z_2 \cdot z_3) = (z_1 \cdot z_2) \cdot z_3$ (Multiplication is always associative)

(iii) Identity : $1 = 1 + i0 \in \mathbb{C}$ is the identity element

(iv) Inverse : Let $z \in \mathbb{C} - \{0\}$. Then $\exists \frac{1}{z} \in \mathbb{C} - \{0\}$ such that $z \cdot \frac{1}{z} = 1 \in \mathbb{C} - \{0\}$.

Solution

Let $G = \mathbb{C} - \{0\}$

(i) Closure : $z_1 \cdot z_2 \in \mathbb{C} \quad \forall\, z_1, z_2 \in \mathbb{C}$

(ii) Associative : Let $z_1, z_2, z_3 \in \mathbb{C}$, then $z_1 \cdot (z_2 \cdot z_3) = (z_1 \cdot z_2) \cdot z_3$ (Multiplication is always associative)

(iii) Identity : $1 = 1 + i0 \in \mathbb{C}$ is the identity element

(iv) Inverse : Let $z \in \mathbb{C} - \{0\}$. Then $\exists \frac{1}{z} \in \mathbb{C} - \{0\}$ such that $z \cdot \frac{1}{z} = 1 \in \mathbb{C} - \{0\}$.

(v) Commutative : $z_1 \cdot z_2 = z_2 \cdot z_1 \ \forall\, z_1, z_2 \in \mathbb{C}$.

Solution

Let $G = \mathbb{C} - \{0\}$

(i) Closure : $z_1 \cdot z_2 \in \mathbb{C} \quad \forall\, z_1, z_2 \in \mathbb{C}$

(ii) Associative : Let $z_1, z_2, z_3 \in \mathbb{C}$, then $z_1 \cdot (z_2 \cdot z_3) = (z_1 \cdot z_2) \cdot z_3$ (Multiplication is always associative)

(iii) Identity : $1 = 1 + i0 \in \mathbb{C}$ is the identity element

(iv) Inverse : Let $z \in \mathbb{C} - \{0\}$. Then $\exists \dfrac{1}{z} \in \mathbb{C} - \{0\}$ such that $z \cdot \dfrac{1}{z} = 1 \in \mathbb{C} - \{0\}$.

(v) Commutative : $z_1 \cdot z_2 = z_2 \cdot z_1 \;\forall\, z_1, z_2 \in \mathbb{C}$.

$\therefore\ \mathbb{C} - \{0\}$ is an abelian group.

Example 4

Show that the set of four matrices $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ form an abelian group, under multiplication of matrices.

Solution

Let $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$
$B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, C = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$

Solution

Let $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$
$B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, C = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$
Let $G = \{I, A, B, C\}$

Solution

Let $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$
$B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, C = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$
Let $G = \{I, A, B, C\}$

·	I	A	B	C
I	I	A	B	C
A	A	I	C	B
B	B	C	I	A
C	C	B	A	I

Solution

Let $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$
$B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, C = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$
Let $G = \{I, A, B, C\}$

·	I	A	B	C
I	I	A	B	C
A	A	I	C	B
B	B	C	I	A
C	C	B	A	I

I is the identity element. Inverse of the each element is itself.

Example 5

Show that the matrices $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ form a a group under matrix multiplication.

Solution

Let $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$

Let $G = \{A, B\}$

Solution

Let $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$

Let $G = \{A, B\}$

(i) Closure :

$$A \cdot B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in G$$

Solution

Let $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$,

Let $G = \{A, B\}$

(i) Closure :

$$A \cdot B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in G$$

(ii) Matrix multiplication is always associative

Solution

Let $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$,

Let $G = \{A, B\}$

(i) Closure :

$$A \cdot B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in G$$

(ii) Matrix multiplication is always associative

(iii) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the multiplicative identity matrix

Solution

Let $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$

Let $G = \{A, B\}$

(i) Closure :

$$A \cdot B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in G$$

(ii) Matrix multiplication is always associative

(iii) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the multiplicative identity matrix

(iv) Inverse of matrix is itself.

Example 6

Show that the set G of all positive rational forms a group under the composition $*$ defined by
$a * b = \frac{ab}{3}$ for all $a, b \in G$.

Solution

(i) Since a, b in positive rational number.

$$\therefore\ a * b = \frac{ab}{3}, \quad \forall a, b \text{ in positive rational.}$$

Solution

(i) Since a, b in positive rational number.

$\therefore\ a * b = \dfrac{ab}{3}, \quad \forall a, b$ in positive rational.

(ii) $a * (b * c) = a * \dfrac{bc}{3} = \dfrac{abc}{3}$

Solution

(i) Since a, b in positive rational number.

$\therefore\ a * b = \frac{ab}{3}, \quad \forall a, b$ in positive rational.

(ii) $a * (b * c) = a * \frac{bc}{3} = \frac{abc}{3}$

$(a * b) * c = \frac{ab}{3} * c = \frac{abc}{3}$

Solution

(i) Since a, b in positive rational number.

$\therefore\ a * b = \dfrac{ab}{3}, \quad \forall a, b$ in positive rational.

(ii) $a * (b * c) = a * \dfrac{bc}{3} = \dfrac{abc}{3}$

$(a * b) * c = \dfrac{ab}{3} * c = \dfrac{abc}{3}$

$\therefore\ a * (b * c) = (a * b) * c$

Solution

(i) Since a, b in positive rational number.

$\therefore\ a * b = \dfrac{ab}{3}, \quad \forall a, b$ in positive rational.

(ii) $a * (b * c) = a * \dfrac{bc}{3} = \dfrac{abc}{3}$

$(a * b) * c = \dfrac{ab}{3} * c = \dfrac{abc}{3}$

$\therefore\ a * (b * c) = (a * b) * c$

(iii) $e = 3$ is the identity element.

Solution

(i) Since a, b in positive rational number.

$\therefore\ a * b = \dfrac{ab}{3}, \quad \forall a, b$ in positive rational.

(ii) $a * (b * c) = a * \dfrac{bc}{3} = \dfrac{abc}{3}$

$(a * b) * c = \dfrac{ab}{3} * c = \dfrac{abc}{3}$

$\therefore\ a * (b * c) = (a * b) * c$

(iii) $e = 3$ is the identity element.

(iv) Let $a \in G$. Then $a^{-1} = \dfrac{9}{a}$.

Example 7

Show that

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}, \begin{pmatrix} \omega^2 & 0 \\ 0 & \omega \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \omega^2 \\ \omega & 0 \end{pmatrix}, \begin{pmatrix} 0 & \omega \\ \omega^2 & 0 \end{pmatrix} \right\},$$

where $\omega^3 = 1, \omega \neq 1$ form a group with respect to matrix multiplication.

Solution

Let $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A = \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}, B = \begin{pmatrix} \omega^2 & 0 \\ 0 & \omega \end{pmatrix},$
$C = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, D = \begin{pmatrix} 0 & \omega^2 \\ \omega & 0 \end{pmatrix}, E = \begin{pmatrix} 0 & \omega \\ \omega^2 & 0 \end{pmatrix}$

Solution

Let $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A = \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}, B = \begin{pmatrix} \omega^2 & 0 \\ 0 & \omega \end{pmatrix},$
$C = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, D = \begin{pmatrix} 0 & \omega^2 \\ \omega & 0 \end{pmatrix}, E = \begin{pmatrix} 0 & \omega \\ \omega^2 & 0 \end{pmatrix}$
Let $G = \{I, A, B, C, D, E\}$

Solution Cont ···

·	I	A	B	C	D	E
I	I	A	B	C	D	E
A	A	B	I	E	C	D
B	B	I	A	D	E	C
C	C	D	E	I	A	B
D	D	E	C	B	I	A
E	E	C	D	A	B	I

Solution Cont · · ·

$\cdot$	I	A	B	C	D	E
I	I	A	B	C	D	E
A	A	B	I	E	C	D
B	B	I	A	D	E	C
C	C	D	E	I	A	B
D	D	E	C	B	I	A
E	E	C	D	A	B	I

From the table

(i) closure is verified

Solution Cont ···

$\cdot$	I	A	B	C	D	E
I	I	A	B	C	D	E
A	A	B	I	E	C	D
B	B	I	A	D	E	C
C	C	D	E	I	A	B
D	D	E	C	B	I	A
E	E	C	D	A	B	I

From the table

(i) closure is verified

(ii) Matrix multiplication is always associative

Solution Cont · · ·

$\cdot$	I	A	B	C	D	E
I	I	A	B	C	D	E
A	A	B	I	E	C	D
B	B	I	A	D	E	C
C	C	D	E	I	A	B
D	D	E	C	B	I	A
E	E	C	D	A	B	I

From the table

(i) closure is verified

(ii) Matrix multiplication is always associative

(iii) I is the identity matrix

Solution Cont $\cdots$

$\cdot$	I	A	B	C	D	E
I	I	A	B	C	D	E
A	A	B	I	E	C	D
B	B	I	A	D	E	C
C	C	D	E	I	A	B
D	D	E	C	B	I	A
E	E	C	D	A	B	I

From the table

(i) closure is verified

(ii) Matrix multiplication is always associative

(iii) I is the identity matrix

(iv) Inverse of I is I,

Solution Cont ⋯

$\cdot$	I	A	B	C	D	E
I	I	A	B	C	D	E
A	A	B	I	E	C	D
B	B	I	A	D	E	C
C	C	D	E	I	A	B
D	D	E	C	B	I	A
E	E	C	D	A	B	I

From the table

(i) closure is verified

(ii) Matrix multiplication is always associative

(iii) I is the identity matrix

(iv) Inverse of I is I, inverse of A is B,

Solution Cont $\cdots$

$\cdot$	I	A	B	C	D	E
I	I	A	B	C	D	E
A	A	B	I	E	C	D
B	B	I	A	D	E	C
C	C	D	E	I	A	B
D	D	E	C	B	I	A
E	E	C	D	A	B	I

From the table

(i) closure is verified

(ii) Matrix multiplication is always associative

(iii) I is the identity matrix

(iv) Inverse of I is I, inverse of A is B, inverse of B is A,

Solution Cont $\cdots$

$\cdot$	I	A	B	C	D	E
I	I	A	B	C	D	E
A	A	B	I	E	C	D
B	B	I	A	D	E	C
C	C	D	E	I	A	B
D	D	E	C	B	I	A
E	E	C	D	A	B	I

From the table

(i) closure is verified

(ii) Matrix multiplication is always associative

(iii) I is the identity matrix

(iv) Inverse of I is I, inverse of A is B, inverse of B is A, inverse of C is C,

Solution Cont $\cdots$

$\cdot$	I	A	B	C	D	E
I	I	A	B	C	D	E
A	A	B	I	E	C	D
B	B	I	A	D	E	C
C	C	D	E	I	A	B
D	D	E	C	B	I	A
E	E	C	D	A	B	I

From the table

(i) closure is verified

(ii) Matrix multiplication is always associative

(iii) I is the identity matrix

(iv) Inverse of I is I, inverse of A is B, inverse of B is A, inverse of C is C, inverse of D is D

Solution Cont ⋯

$\cdot$	I	A	B	C	D	E
I	I	A	B	C	D	E
A	A	B	I	E	C	D
B	B	I	A	D	E	C
C	C	D	E	I	A	B
D	D	E	C	B	I	A
E	E	C	D	A	B	I

From the table

(i) closure is verified

(ii) Matrix multiplication is always associative

(iii) I is the identity matrix

(iv) Inverse of I is I, inverse of A is B, inverse of B is A, inverse of C is C, inverse of D is D and inverse of E is E.

Example 8

Show that the set $G = \{2^n / n \in \mathbb{Z}\}$ is an abelian group under multiplication.

Solution

$G = \{2^n / n \in \mathbb{Z}\}$ to show that $(G, .)$ is an abelian group.

Solution

$G = \{2^n / n \in \mathbb{Z}\}$ to show that $(G, .)$ is an abelian group.

(i) Let $a = 2^n, b = 2^m$ then
$a \cdot b = 2^n \cdot 2^m = 2^{n+m} \in G$

Solution

$G = \{2^n / n \in \mathbb{Z}\}$ to show that $(G, .)$ is an abelian group.

(i) Let $a = 2^n, b = 2^m$ then
$a \cdot b = 2^n \cdot 2^m = 2^{n+m} \in G$

(ii) Associative property is satisfied.

Solution

$G = \{2^n / n \in \mathbb{Z}\}$ to show that $(G, .)$ is an abelian group.

(i) Let $a = 2^n, b = 2^m$ then
$a \cdot b = 2^n \cdot 2^m = 2^{n+m} \in G$

(ii) Associative property is satisfied.

(iii) 1 is the identity element.

Solution

$G = \{2^n / n \in \mathbb{Z}\}$ to show that $(G, .)$ is an abelian group.

(i) Let $a = 2^n, b = 2^m$ then
$a \cdot b = 2^n \cdot 2^m = 2^{n+m} \in G$

(ii) Associative property is satisfied.

(iii) 1 is the identity element.

(iv) Inverse of 2^n is 2^{-n}

Solution

$G = \{2^n / n \in \mathbb{Z}\}$ to show that $(G, .)$ is an abelian group.

(i) Let $a = 2^n, b = 2^m$ then
$a \cdot b = 2^n \cdot 2^m = 2^{n+m} \in G$

(ii) Associative property is satisfied.

(iii) 1 is the identity element.

(iv) Inverse of 2^n is 2^{-n}

(v) Commutative is obvious.

Solution

$G = \{2^n / n \in \mathbb{Z}\}$ to show that $(G, .)$ is an abelian group.

(i) Let $a = 2^n, b = 2^m$ then
$a \cdot b = 2^n \cdot 2^m = 2^{n+m} \in G$

(ii) Associative property is satisfied.

(iii) 1 is the identity element.

(iv) Inverse of 2^n is 2^{-n}

(v) Commutative is obvious.

Example 9

Prove that $< S, \cdot >$ where $S = \{1, \omega, \omega^2\}$ $1, \omega, \omega^2$ are cube roots of unity is a finite abelian group.

Solution

Let $S = \{1, \omega, \omega^2\}$

Solution

Let $S = \{1, \omega, \omega^2\}$

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

Solution

Let $S = \{1, \omega, \omega^2\}$

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

(i) Closure, Associative, commutative obvious.

Solution

Let $S = \{1, \omega, \omega^2\}$

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

(i) Closure, Associative, commutative obvious.

(ii) Identity is 1

Solution

Let $S = \{1, \omega, \omega^2\}$

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

(i) Closure, Associative, commutative obvious.

(ii) Identity is 1

(iii) Inverse of 1 is 1, inverse of ω is ω^2 and inverse of ω^2 is ω.

Solution

Let $S = \{1, \omega, \omega^2\}$

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

(i) Closure, Associative, commutative obvious.

(ii) Identity is 1

(iii) Inverse of 1 is 1, inverse of ω is ω^2 and inverse of ω^2 is ω.

Example 10

Prove that $< S, . >$ where $S = \{1, -1, i, -i\}$ is a set of fourth roots of unity, is a group where $i^2 = -1$.

Solution

$S = \{1, -1, i, -i\}$

Solution

$S = \{1, -1, i, -i\}$

*	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

Solution

$S = \{1, -1, i, -i\}$

$*$	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

(i) The identity element is 1.

Solution

$S = \{1, -1, i, -i\}$

$*$	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

(i) The identity element is 1.

(ii) The inverse of 1 is 1, inverse of $1, i, -1$ and $-i$ are $1, -i, -1$ and i respectively.

Problems

Question 1

The set of all real numbers under the usual multiplication operation is not a group since

Question 1

The set of all real numbers under the usual multiplication operation is not a group since

Answer Key

(a) multiplication is not a binary operation

(b) multiplication is not associative

(c) identity element does not exist

(d) zero has no inverse

Question 1

The set of all real numbers under the usual multiplication operation is not a group since

Answer Key

(a) multiplication is not a binary operation
(b) multiplication is not associative
(c) identity element does not exist
(d) zero has no inverse

Answer is

The correct choice is (d) zero has no inverse

Question 2

If $(G, \cdot)$ is a group such that
$(ab)^{-1} = a^{-1}b^{-1}, \forall a, b \in G$, then G is a / an

Question 2

If $(G, \cdot)$ is a group such that $(ab)^{-1} = a^{-1}b^{-1}, \forall a, b \in G$, then G is a / an

Answer Key

(a) commutative semi group
(b) abelian group
(c) non - abelian group
(d) None of these

Question 2

If $(G, \cdot)$ is a group such that
$(ab)^{-1} = a^{-1}b^{-1}, \forall a, b \in G$, then G is a / an

Answer Key

(a) commutative semi group
(b) abelian group
(c) non - abelian group
(d) None of these

Answer is

The correct choice is
(b) Abelian group

Question 3

The inverse of $-i$ in the multiplicative group, $\{1, -1, i, -i\}$ is

Question 3

The inverse of $-i$ in the multiplicative group, $\{1, -1, i, -i\}$ is

Answer Key

(a) 1
(b) -1
(c) i
(d) -i

Question 3

The inverse of $-i$ in the multiplicative group, $\{1, -1, i, -i\}$ is

Answer Key

(a) 1
(b) -1
(c) i
(d) -i

Answer is

The correct choice is (c) i

Question 4

The set of integers $\mathbb{Z}$ with the binary operation $*$ defined as $a * b = a + b + 1$ for $a, b \in \mathbb{Z}$, is a group. The identity element of this group is

Question 4

The set of integers $\mathbb{Z}$ with the binary operation $*$ defined as $a * b = a + b + 1$ for $a, b \in \mathbb{Z}$, is a group. The identity element of this group is

Answer Key

(a) 0

(b) 1

(c) -1

(d) 12

Question 4

The set of integers $\mathbb{Z}$ with the binary operation $*$ defined as $a * b = a + b + 1$ for $a, b \in \mathbb{Z}$, is a group. The identity element of this group is

Answer Key

(a) 0

(b) 1

(c) -1

(d) 12

Answer is

The correct choice is (c) -1

Question 5

In the group $(G, \cdot)$, the value of $(a^{-1}b)^{-1}$ is

Question 5

In the group $(G, \cdot)$, the value of $(a^{-1}b)^{-1}$ is

Answer Key

(a) ab^{-1}
(b) $b^{-1}a$
(c) $a^{-1}b$
(d) ba^{-1}

Question 5

In the group $(G, \cdot)$, the value of $(a^{-1}b)^{-1}$ is

Answer Key

(a) ab^{-1}

(b) $b^{-1}a$

(c) $a^{-1}b$

(d) ba^{-1}

Answer is

The correct choice is (b) $b^{-1}a$

Question 6

If $(G, \cdot)$ is a group, such that $(ab)^2 = a^2b^2 \, \forall \, a, b \in G$, then G is a / an

Question 6

If $(G, \cdot)$ is a group, such that $(ab)^2 = a^2 b^2 \,\forall\, a, b \in G$, then G is a / an

Answer Key

(a) commutative semi group
(b) abelian group
(c) non - abelian group
(d) None of these

Question 6

If $(G, \cdot)$ is a group, such that $(ab)^2 = a^2 b^2 \, \forall \, a, b \in G$, then G is a / an

Answer Key

(a) commutative semi group
(b) abelian group
(c) non - abelian group
(d) None of these

Answer is

The correct choice is (b) abelian group

Question 7

$(\mathbb{Z}, *)$ is a group with $a * b = a + b + 1 \, \forall \, a, b \in \mathbb{Z}$.
The inverse of a is

Question 7

$(\mathbb{Z}, *)$ is a group with $a * b = a + b + 1 \, \forall \, a, b \in \mathbb{Z}$. The inverse of a is

Answer Key

(a) 0
(b) -2
(c) $a - 2$
(d) $-a - 2$

Question 7

$(\mathbb{Z}, *)$ is a group with $a * b = a + b + 1 \, \forall \, a, b \in \mathbb{Z}$.
The inverse of a is

Answer Key

(a) 0
(b) -2
(c) $a - 2$
(d) $-a - 2$

Answer is

The correct choice is
(d) $-a - 2$

❁❁❁ Time to Interact ❁❁❁


Thank You