AL FM Discrete

Group Theory

T. Bretschneider

April 15, 2021

Outline

What is a Group? I

Definition

A non-empty set G with binary operation $*$ is said to be a **group**, written $(G, *)$, if each of the following four axioms hold:

- G is **closed** under $*$ (for all $a, b \in G, a * b \in G$)
- $*$ is **associative** on G (for all $a, b, c \in G, (a * b) * c = a * (b * c)$)
- $*$ has an **identity** element in G (there exists $e \in G$ such that $a * e = e * a = a$ for all $a \in G$)
- Each element of G has an **inverse** under $*$ (for each $a \in G$ there exists a^{-1} so $a^{-1} * a = a * a^{-1} = e$)

Definition

The number of elements in a group is called the **order of the group**.

It is possible to have groups with infinite order, e.g. $(\mathbb{Z}, +)$ (the set of all integers under addition)

Problem

The set $A = w, x, y, z$. The Cayley table shows the outcome for each pair of elements of the set A under the binary operation $*$.
Prove that the set A forms a group under the binary

$*$	w	x	y	z
w	w	x	y	z
x	x	w	z	y
y	y	z	x	w

What is a Group? II

Closure: The Cayley table only contains elements of A and so A is closed on $*$.
Identity: w is the identity as the row and column is a copy of the header row and column.
Inverse: As there is the identity in each row and column, each element has an inverse.

Test Your Understanding

Problem

Prove that the set of non-negative integers does not form a group under the binary operation of addition.

Problem

A student says that the set $A = 2, 5, 8, 10$ forms a group under multiplication modulo 15. Determine whether the student is correct.

Problem

Let $G = \mathbb{Q}^+$ with binary operation $*$ where $a * b = \frac{ab}{4}$ where $a, b \in \mathbb{Q}^+$. Show that $(G, *)$ is a group.

Test Your Understanding

Problem

Prove that the set of non-negative integers does not form a group under the binary operation of addition.

The Identity element under addition is zero which is a non-negative integer.
However none of the other elements have an inverse in the group (as the inverse of an element a would be $-a$, a negative integer)

Problem

A student says that the set $A = 2, 5, 8, 10$ forms a group under multiplication modulo 15. Determine whether the student is correct.

Problem

Let $G = \mathbb{Q}^+$ with binary operation $*$ where $a * b = \frac{ab}{4}$ where $a, b \in \mathbb{Q}^+$. Show that $(G, *)$ is a group.

Test Your Understanding

Problem

Prove that the set of non-negative integers does not form a group under the binary operation of addition.

The Identity element under addition is zero which is a non-negative integer.
However none of the other elements have an inverse in the group (as the inverse of an element a would be $-a$, a negative integer)

Problem

A student says that the set $A = 2, 5, 8, 10$ forms a group under multiplication modulo 15. Determine whether the student is correct.

A is not closed under multiplication modulo 15 because $2 \times_{15} 8 = 1 \notin A$

Problem

Let $G = \mathbb{Q}^+$ with binary operation $*$ where $a * b = \frac{ab}{4}$ where $a, b \in \mathbb{Q}^+$. Show that $(G, *)$ is a group.

Test Your Understanding

Problem

Prove that the set of non-negative integers does not form a group under the binary operation of addition.

The Identity element under addition is zero which is a non-negative integer.
However none of the other elements have an inverse in the group (as the inverse of an element a would be $-a$, a negative integer)

Problem

A student says that the set $A = 2, 5, 8, 10$ forms a group under multiplication modulo 15. Determine whether the student is correct.

A is not closed under multiplication modulo 15 because $2 \times_{15} 8 = 1 \notin A$

Problem

Let $G = \mathbb{Q}^+$ with binary operation $*$ where $a * b = \frac{ab}{4}$ where $a, b \in \mathbb{Q}^+$. Show that $(G, *)$ is a group.

Closure: If $a, b \in \mathbb{Q}^+$ then $a = \frac{p}{q}$ and $b = \frac{r}{s}$ where $p, q, r, s \in \mathbb{Z}$, $a * b = \frac{pr}{4qs} \in \mathbb{Q}^+$.
Associativity: Follows from the associativity of multiplication in $\mathbb{R}$.
Identity: $a * 4 = \frac{a \times \mathbf{4}}{4} = a$, and commutativity follows from commutativity of multiplication in $\mathbb{R}$, so the identity is 4, which is in $\mathbb{Q}^+$.

Past Paper Question

Problem

The set M is defined as

$$M = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} : \theta \in \mathbb{R} \right\}.$$

Prove that M forms a group under the operation of matrix multiplication.

Past Paper Question

Problem

The set M is defined as

$$M = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} : \theta \in \mathbb{R} \right\}.$$

Prove that M forms a group under the operation of matrix multiplication.

Closure:

$$\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix} =$$

$$= \begin{pmatrix} \cos\alpha\cos\beta - \sin\alpha\sin\beta & -(\cos\alpha\sin\beta + \sin\alpha\cos\beta) \\ \sin\alpha\cos\beta + \cos\alpha\sin\beta & \cos\alpha\cos\beta - \sin\alpha\sin\beta \end{pmatrix}$$

$$\begin{pmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{pmatrix}$$

Associativity: Follows from associativity of matrix multiplication.
Identity: Follows from matrix identity. Which is part of M, when $\theta = 0$.
Inverse: Set $\beta = \alpha$ and result follows.

Period (or Order) of an Element

Definition

The **period (or Order) of an element** a of a group $(G, *)$ is the smallest n such that $a^n = e$

Problem

For the group shown by the Clayley table:

- *State the identity element*
- *Find the period (or order) of each element.*

Period (or Order) of an Element

Definition

The **period (or Order) of an element** a of a group $(G, *)$ is the smallest n such that $a^n = e$

Problem

For the group shown by the Clayley table:

- *State the identity element*
- *Find the period (or order) of each element.*

The identity element is I

Period (or Order) of an Element

Definition

The **period (or Order) of an element** a of a group $(G, *)$ is the smallest n such that $a^n = e$

Problem

For the group shown by the Clayley table:

- *State the identity element*
- *Find the period (or order) of each element.*

The identity element is I
The order of I is 1
The orders of X, Y, Z are 2, as they are all self-inverse.

Abelian Groups

Definition

If a group $(G, *)$ also has the property that $*$ is commutative the it is an **Abelian Group**.

Problem

The Cayley table shows a group that is called the Quaternion group:

- *What is the order of the group?*
- *What is the identity element?*
- *What is the period of the element $-k$?*
- *Is the Quaternion group Abelian? Justify your answer.*

Abelian Groups

Definition

If a group $(G, *)$ also has the property that $*$ is commutative the it is an **Abelian Group**.

Problem

The Cayley table shows a group that is called the Quaternion group:

- *What is the order of the group?*
- *What is the identity element?*
- *What is the period of the element $-k$?*
- *Is the Quaternion group Abelian? Justify your answer.*

The order of the group is 8

Abelian Groups

Definition

If a group $(G, *)$ also has the property that $*$ is commutative the it is an **Abelian Group**.

Problem

The Cayley table shows a group that is called the Quaternion group:

- *What is the order of the group?*
- *What is the identity element?*
- *What is the period of the element $-k$?*
- *Is the Quaternion group Abelian? Justify your answer.*

The order of the group is 8 The Identity element is 1

Abelian Groups

Definition

If a group $(G, *)$ also has the property that $*$ is commutative the it is an **Abelian Group**.

Problem

The Cayley table shows a group that is called the Quaternion group:

- *What is the order of the group?*
- *What is the identity element?*
- *What is the period of the element $-k$?*
- *Is the Quaternion group Abelian? Justify your answer.*

The order of the group is 8 The Identity element is 1
$-k^1 = -k, -k^2 = -1, -k^3 = k, -k^4 = 1$. Therefore $-k$ has period 4.

Abelian Groups

Definition

If a group $(G, *)$ also has the property that $*$ is commutative the it is an **Abelian Group**.

Problem

The Cayley table shows a group that is called the Quaternion group:

- *What is the order of the group?*
- *What is the identity element?*
- *What is the period of the element $-k$?*
- *Is the Quaternion group Abelian? Justify your answer.*

The order of the group is 8 The Identity element is 1
$-k^1 = -k, -k^2 = -1, -k^3 = k, -k^4 = 1$. Therefore $-k$ has period 4. $j * k = -i$ and $k * j = i$ so $j * k \neq k * j$ and so the Quaternion group is not Abelian.

Test Your Understanding

Problem

Show that $\{1, 2, 3, 4\}$ *form an Abelian group under* $\times_5$

Problem

Prove that $\{a + bi : a, b \in \mathbb{R}, |a + bi| = 1\}$ *forms an Abelian group under multiplication.*

Test Your Understanding

Problem

Show that $\{1, 2, 3, 4\}$ *form an Abelian group under* $\times_5$

The Cayley table is :
Closure: Since the only elements in the Cayley table are in the set then it is closed.
Associativity: Follows from the associativity of multiplication on $\mathbb{R}$.
Identity: 1 is the identity as it leaves the header row and column of the Cayley table unchanged.
Inverse: Since the identity element, 1, is in each row and column, every element has an inverse.
Commutativity: The Cayley table is symmetrical around the leading diagonal.

Problem

Prove that $\{a + bi : a, b \in \mathbb{R}, |a + bi| = 1\}$ *forms an Abelian group under multiplication.*

Test Your Understanding

Problem

Show that $\{1, 2, 3, 4\}$ *form an Abelian group under* $\times_5$

The Cayley table is :
Closure: Since the only elements in the Cayley table are in the set then it is closed.
Associativity: Follows from the associativity of multiplication on $\mathbb{R}$.
Identity: 1 is the identity as it leaves the header row and column of the Cayley table unchanged.
Inverse: Since the identity element, 1, is in each row and column, every element has an inverse.
Commutativity: The Cayley table is symmetrical around the leading diagonal.

Problem

Prove that $\{a + bi : a, b \in \mathbb{R}, |a + bi| = 1\}$ *forms an Abelian group under multiplication.*

$a + bi$ can in this case be written as $e^{i\theta}$.
Closure: $e^{i\alpha} \times e^{i\beta} = e^{i(\alpha+\beta)}$ which is clearly also in the group.
Associativity: Follows from the associativity of multiplication on $\mathbb{C}$.
Identity: 1 is the multiplicative identity. Which is also in the group.
Inverse: $e^{i\alpha} \times e^{i(-\alpha)} = e^0 = 1$ and $e^{-i\alpha}$ is clearly in the group.
Commutativity: Follows from commutativity of multiplication on $\mathbb{C}$

Subgroups

Definition

Given a group $(G, *)$, if H is a non-empty subset of G which is also a group under the binary operation $*$ then we say that H is a **subgroup** of G.

Consider the group $\{0, 1, 2, 3, 4, 5\}$ under $+_6$:
Consider the subsets $\{0, 2, 4\}$ and $\{0, 3\}$ of the set. If we form the Cayley table using just these elements, it can be shown that both of these are groups in their own right, and therefore subgroups of the original group.

Trivial, Non-Trivial and Proper Subgroups

Definition

The group containing just the identity element will always be a subgroup. We call this the **trivial subgroup**.

Definition

Other subgroups are called **non-trivial** subgroups.

Definition

Any set is a subset of itself and therefore technically any group is a subgroup of itself. A **proper subgroup** is any subgroup which is not the parent group itself.

Problem

A group G is formed by the set $A = \{w, x, y, z\}$ under the binary operation $*$ with outcomes as shown in the Cayley table.

- *State the proper subgroups of $(G, *)$*
- *State the non-trivial subgroups of $(G, *)$*

Trivial, Non-Trivial and Proper Subgroups

Definition

The group containing just the identity element will always be a subgroup. We call this the **trivial subgroup**.

Definition

Other subgroups are called **non-trivial** subgroups.

Definition

Any set is a subset of itself and therefore technically any group is a subgroup of itself. A **proper subgroup** is any subgroup which is not the parent group itself.

Problem

A group G is formed by the set $A = \{w, x, y, z\}$ under the binary operation $*$ with outcomes as shown in the Cayley table.

- *State the proper subgroups of $(G, *)$*
- *State the non-trivial subgroups of $(G, *)$*

w and $\{w, x\}$ are subsets of A which would form proper subgroups of $(G, *)$.

Trivial, Non-Trivial and Proper Subgroups

Definition

The group containing just the identity element will always be a subgroup. We call this the **trivial subgroup**.

Definition

Other subgroups are called **non-trivial** subgroups.

Definition

Any set is a subset of itself and therefore technically any group is a subgroup of itself. A **proper subgroup** is any subgroup which is not the parent group itself.

Problem

A group G is formed by the set $A = \{w, x, y, z\}$ under the binary operation $*$ with outcomes as shown in the Cayley table.

- *State the proper subgroups of $(G, *)$*
- *State the non-trivial subgroups of $(G, *)$*

w and $\{w, x\}$ are subsets of A which would form proper subgroups of $(G, *)$.
$\{w, x\}$ and $\{w, x, y, z\}$ are subsets of A which would form non-trivial subgroups of G under $*$.

Trivial, Non-Trivial and Proper Subgroups

Definition

The group containing just the identity element will always be a subgroup. We call this the **trivial subgroup**.

Definition

Other subgroups are called **non-trivial** subgroups.

Definition

Any set is a subset of itself and therefore technically any group is a subgroup of itself. A **proper subgroup** is any subgroup which is not the parent group itself.

Problem

A group G is formed by the set $A = \{w, x, y, z\}$ under the binary operation $*$ with outcomes as shown in the Cayley table.

- *State the proper subgroups of $(G, *)$*
- *State the non-trivial subgroups of $(G, *)$*

w and $\{w, x\}$ are subsets of A which would form proper subgroups of $(G, *)$.
$\{w, x\}$ and $\{w, x, y, z\}$ are subsets of A which would form non-trivial subgroups of G under $*$.

Cyclic Groups

Definition

A group $(G, *)$ is **cyclic** if every element can be written as a^n for some $a \in G$ and $n \in Z$.

In other words, if you can generate the whole group using just one element and the binary operator then it is cyclic.

Definition

Any element, a, of a cyclic group where any element can be written as a^n for some $n \in \mathbb{Z}$ is called a generator of that cyclic group.

It is possible for a cyclic group to be infinite. For instance, $(\mathbb{Z}, +)$ is cyclic as it can be generated by 1.

Problem

What are the generators of the cyclic group $(\{1, -1, i, -i\}, \times)$*?*

Cyclic Groups

Definition

A group $(G, *)$ is **cyclic** if every element can be written as a^n for some $a \in G$ and $n \in Z$.

In other words, if you can generate the whole group using just one element and the binary operator then it is cyclic.

Definition

Any element, a, of a cyclic group where any element can be written as a^n for some $n \in \mathbb{Z}$ is called a generator of that cyclic group.

It is possible for a cyclic group to be infinite. For instance, $(\mathbb{Z}, +)$ is cyclic as it can be generated by 1.

Problem

What are the generators of the cyclic group $(\{1, -1, i, -i\}, \times)$*?*

$i^1 = i, i^2 = -1, i^3 = -i, i^4 = 1$. Therefore i is a generator. By similar reasoning $-i$ is also a generator.

Test Your Understanding

Problem

Show that the group $(\{1, 2, 3, 4, 5, 6\}, \times_7)$ *is a cyclic group.*

Test Your Understanding

Problem

Show that the group $(\{1, 2, 3, 4, 5, 6\}, \times_7)$ *is a cyclic group.*

Closure: The Cayley table only contains elements from the set so it is closed.
Associativity: Follows from the associativity of multiplication on $\mathbb{R}$.
Identity: 1 is the identity as the 1 row and column leave the header row and column unchanged.
Inverse: There is a 1 in every row and column so there is an inverse for each element.
$3^1 = 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1$
Therefore 3 is a generator and so the group is cyclic.

Test Your Understanding

Problem

M is the set of all 2×2 invertible matrices.

- *Show that M forms a group under the binary operation of matrix multiplication.*
- *State whether or not M is an Abelian group.*
- *Show that the set $N = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$ is a subgroup of the group M under the binary operation of matrix multiplication.*

Test Your Understanding

Problem

M is the set of all 2×2 invertible matrices.

- *Show that M forms a group under the binary operation of matrix multiplication.*
- *State whether or not M is an Abelian group.*
- *Show that the set $N = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$ is a subgroup of the group M under the binary operation of matrix multiplication.*

Test Your Understanding

Problem

M is the set of all 2×2 invertible matrices.

- *Show that M forms a group under the binary operation of matrix multiplication.*
- *State whether or not M is an Abelian group.*
- *Show that the set $N = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$ is a subgroup of the group M under the binary operation of matrix multiplication.*

Closure: Since $\det AB = \det(A)\det(B)$ then if $\det A, \det B \neq 0, \det AB \neq 0$. So $AB \in M$.
Associativity: Matrix multiplication is associative.
Identity: The identity matrix is in M.
Inverse: A^{-1} will be in M since $\det A^{-1} = \frac{1}{\det A}$.

Test Your Understanding

Problem

M is the set of all 2×2 invertible matrices.

- *Show that M forms a group under the binary operation of matrix multiplication.*
- *State whether or not M is an Abelian group.*
- *Show that the set $N = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$ is a subgroup of the group M under the binary operation of matrix multiplication.*

Closure: Since $\det AB = \det(A)\det(B)$ then if $\det A, \det B \neq 0, \det AB \neq 0$. So $AB \in M$.
Associativity: Matrix multiplication is associative.
Identity: The identity matrix is in M.
Inverse: A^{-1} will be in M since $\det A^{-1} = \frac{1}{\det A}$.
Matrix multiplication is not commutative so the group will not be Abelian.

Test Your Understanding

Problem

M is the set of all 2×2 invertible matrices.

- *Show that M forms a group under the binary operation of matrix multiplication.*
- *State whether or not M is an Abelian group.*
- *Show that the set $N = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$ is a subgroup of the group M under the binary operation of matrix multiplication.*

Closure: Since $\det AB = \det(A)\det(B)$ then if $\det A, \det B \neq 0, \det AB \neq 0$. So $AB \in M$.
Associativity: Matrix multiplication is associative.
Identity: The identity matrix is in M.
Inverse: A^{-1} will be in M since $\det A^{-1} = \frac{1}{\det A}$.
Matrix multiplication is not commutative so the group will not be Abelian.
Closure: $I^2 = I, I \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} I = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = I.$
Thus closed under matrix multiplication.
Associativity: Follows from parent group.

Generators

Definition

A cyclic subgroup can always be formed by picking one element of the parent group and using it to generate a group.
We denote as $< a >$ the group generated by the element a.

Problem

Determine the order of the group $(< 2 >, +_7)$.

Problem

The group R *is defined as* $R = (< 4 >, \times_7)$. *Construct a Cayley table for* R.

Generators

Definition

A cyclic subgroup can always be formed by picking one element of the parent group and using it to generate a group.
We denote as $< a >$ the group generated by the element a.

Problem

Determine the order of the group $(< 2 >, +_7)$.

$2^1 = 2, 2^2 = 4, 2^3 = 6, 2^4 = 1, 2^5 = 3, 2^6 = 5, 2^7 = 0$, which is the identity.
Therefore the group has order 7.

Problem

The group R is defined as $R = (< 4 >, \times_7)$. Construct a Cayley table for R.

Generators

Definition

A cyclic subgroup can always be formed by picking one element of the parent group and using it to generate a group.
We denote as $< a >$ the group generated by the element a.

Problem

Determine the order of the group $(< 2 >, +_7)$.

$2^1 = 2, 2^2 = 4, 2^3 = 6, 2^4 = 1, 2^5 = 3, 2^6 = 5, 2^7 = 0$, which is the identity.
Therefore the group has order 7.

Problem

The group R is defined as $R = (< 4 >, \times_7)$. Construct a Cayley table for R.

aoeu

Past Paper Question

Problem

The set $\{1, 2, 4, , 8, 9, 13, 15, 16\}$ *forms a group under the operation of multiplication modulo 17.*
Which of the following is a generator of the group?

- *4*
- *9*
- *13*
- *16*

Past Paper Question

Problem

The set $\{1, 2, 4, , 8, 9, 13, 15, 16\}$ *forms a group under the operation of multiplication modulo 17.*
Which of the following is a generator of the group?

- *4*
- *9*
- *13*
- *16*

9

Rotational Symmetries of Regular Polygons

Consider the anti-clockwise rotational symmetries of an equilateral triangle.
Let r be an anticlockwise rotation of 120 degrees, then r^2 is a rotation of 240 degrees.
Let e be the identity rotation of leaving it as it is.
Then the Cayley table is as follows:
This is closed, has an identity and each element has an inverse and therefore it is a group.
If fact it is a cyclic group with generator r (or r^2).
The same is true for any regular polygon.

Rotation and Reflection Symmetries

There are six rotation of reflection symmetries of an equilateral triangle:

- e the identity transformation
- r rotate anticlockwise by 120 degrees
- r^2 rotate anticlockwise by 240 degrees
- x reflect in the line L_1
- y reflect in the line L_2
- z reflect in the line L_3

This gives the following Cayley table:
This is closed, associative, has an identity and each element has an inverse and therefore is a group.

Definition

This group is called the **dihedral** group of order 6. There is a similar **dihedral** group of order $2n$ for an n-sided regular polygon.

Test Your Understanding

Problem

- *Find the Cayley table for the symmetries of a rectangle. You should let R_1 and R_2 be the two reflection and have r denote a rotation of 180 degrees.*
- *Prove that the set of symmetries of a rectangle forms a group.*
  You may assume that composition of transformation is associative.
- *Give the period of each of the elements.*
- *State whether the group is Abelian.*

Test Your Understanding

Problem

- *Find the Cayley table for the symmetries of a rectangle. You should let R_1 and R_2 be the two reflection and have r denote a rotation of 180 degrees.*
- *Prove that the set of symmetries of a rectangle forms a group.*
  You may assume that composition of transformation is associative.
- *Give the period of each of the elements.*
- *State whether the group is Abelian.*

The table!!

Test Your Understanding

Problem

- *Find the Cayley table for the symmetries of a rectangle. You should let R_1 and R_2 be the two reflection and have r denote a rotation of 180 degrees.*
- *Prove that the set of symmetries of a rectangle forms a group. You may assume that composition of transformation is associative.*
- *Give the period of each of the elements.*
- *State whether the group is Abelian.*

The table!!
Closure: Each element of the Cayley table is one of the original symmetries.
Associativity: The question lets us assume this.
Identity: The row and column for the transformation e is the same as the header row and column.
Inverse: The identity appears in every row and column, so every element has an inverse.

Test Your Understanding

Problem

- *Find the Cayley table for the symmetries of a rectangle. You should let R_1 and R_2 be the two reflection and have r denote a rotation of 180 degrees.*
- *Prove that the set of symmetries of a rectangle forms a group. You may assume that composition of transformation is associative.*
- *Give the period of each of the elements.*
- *State whether the group is Abelian.*

The table!!
Closure: Each element of the Cayley table is one of the original symmetries.
Associativity: The question lets us assume this.
Identity: The row and column for the transformation e is the same as the header row and column.
Inverse: The identity appears in every row and column, so every element has an inverse.
$|e| = 1, |r| = 2, |R_1| = 2$ *and* $|R_2| = 2$

Test Your Understanding

Problem

- *Find the Cayley table for the symmetries of a rectangle. You should let R_1 and R_2 be the two reflection and have r denote a rotation of 180 degrees.*
- *Prove that the set of symmetries of a rectangle forms a group.*
  You may assume that composition of transformation is associative.
- *Give the period of each of the elements.*
- *State whether the group is Abelian.*

The table!!
Closure: Each element of the Cayley table is one of the original symmetries.
Associativity: The question lets us assume this.
Identity: The row and column for the transformation e is the same as the header row and column.
Inverse: The identity appears in every row and column, so every element has an inverse.
$|e| = 1, |r| = 2, |R_1| = 2$ *and* $|R_2| = 2$
The Cayley table is symmetrical about the leading diagonal so the group is Abelian.

Lagrange's Theorem

Theorem

The order of any subgroup must divide the order of the parent group.

Problem

Determine the only possible orders of the subgroups of a group that has order 81.

Problem

Prove that no subgroups of order 12 exist for a group of order 196

Problem

A student states that $(\{1, -1, i\}, \times)$ *is a subgroup of the group* $(\{1, -1, i, -i\}, \times)$. *Explain whether the student is correct, fully justifying your answer.*

Lagrange's Theorem

Theorem

The order of any subgroup must divide the order of the parent group.

Problem

Determine the only possible orders of the subgroups of a group that has order 81.

$81 = 3^4$, so only factors of 81 are 1,3,9,27,81.
So by Lagrange's Theorem these are the only possible orders of any subgroups.

Problem

Prove that no subgroups of order 12 exist for a group of order 196

Problem

A student states that $(\{1, -1, i\}, \times)$ *is a subgroup of the group* $(\{1, -1, i, -i\}, \times)$.
Explain whether the student is correct, fully justifying your answer.

Lagrange's Theorem

Theorem

The order of any subgroup must divide the order of the parent group.

Problem

Determine the only possible orders of the subgroups of a group that has order 81.

$81 = 3^4$, so only factors of 81 are 1,3,9,27,81.
So by Lagrange's Theorem these are the only possible orders of any subgroups.

Problem

Prove that no subgroups of order 12 exist for a group of order 196

12 does not divide 196, so by Lagrange's Theorem there cannot be any subgroups of order 12.

Problem

A student states that $(\{1, -1, i\}, \times)$ *is a subgroup of the group* $(\{1, -1, i, -i\}, \times)$. *Explain whether the student is correct, fully justifying your answer.*

Lagrange's Theorem

Theorem

The order of any subgroup must divide the order of the parent group.

Problem

Determine the only possible orders of the subgroups of a group that has order 81.

$81 = 3^4$, so only factors of 81 are 1,3,9,27,81.
So by Lagrange's Theorem these are the only possible orders of any subgroups.

Problem

Prove that no subgroups of order 12 exist for a group of order 196

12 does not divide 196, so by Lagrange's Theorem there cannot be any subgroups of order 12.

Problem

A student states that $(\{1, -1, i\}, \times)$ *is a subgroup of the group* $(\{1, -1, i, -i\}, \times)$. *Explain whether the student is correct, fully justifying your answer.*

Since 3 does not divide 4, a group of order 4 cannot have a subgroup of order 3, as in this case.

Past Paper Question

Problem

The group $(G, *)$ has order 8. q and r are elements of G, with the following properties:

$$r \text{ has period } 4$$

$$q \text{ has period } 2$$

$$r^3 * q = q * r$$

- *Explain why $(G, *)$ is not an abelian group.*
- *Show that*
$$r^2 * q * r^2 = q.$$
- *Jenny claims that the **only** possible orders of the subgroups of G are 2,3,4,5,6 and 7 because each of these numbers is less than the order of G.*
Comment fully on the validity of Jenny's claim.
Fully justify your answer.

Past Paper Question

Problem

The group $(G, *)$ has order 8. q and r are elements of G, with the following properties:

$$r \text{ has period } 4$$

$$q \text{ has period } 2$$

$$r^3 * q = q * r$$

- *Explain why $(G, *)$ is not an abelian group.*
- *Show that*
$$r^2 * q * r^2 = q.$$
- *Jenny claims that the **only** possible orders of the subgroups of G are 2,3,4,5,6 and 7 because each of these numbers is less than the order of G.*
Comment fully on the validity of Jenny's claim.
Fully justify your answer.

$q * r = r^3 * q \neq r * q$. Hence not commutative and hence the group won't be abelian.

Past Paper Question

Problem

The group $(G, *)$ has order 8. q and r are elements of G, with the following properties:

$$r \text{ has period } 4$$

$$q \text{ has period } 2$$

$$r^3 * q = q * r$$

- *Explain why $(G, *)$ is not an abelian group.*
- *Show that*
$$r^2 * q * r^2 = q.$$
- *Jenny claims that the **only** possible orders of the subgroups of G are 2,3,4,5,6 and 7 because each of these numbers is less than the order of G.*
Comment fully on the validity of Jenny's claim.
Fully justify your answer.

$q * r = r^3 * q \neq r * q$. Hence not commutative and hence the group won't be abelian.
$r^2 * q * r^2 = r^2 * r^3 * q * r = r * q * r = r * r^3 * q = q$. As required.

Past Paper Question

Problem

The group $(G, *)$ has order 8. q and r are elements of G, with the following properties:

$$r \text{ has period } 4$$

$$q \text{ has period } 2$$

$$r^3 * q = q * r$$

- *Explain why $(G, *)$ is not an abelian group.*
- *Show that*
$$r^2 * q * r^2 = q.$$
- *Jenny claims that the **only** possible orders of the subgroups of G are 2,3,4,5,6 and 7 because each of these numbers is less than the order of G.*
Comment fully on the validity of Jenny's claim.
Fully justify your answer.

$q * r = r^3 * q \neq r * q$. Hence not commutative and hence the group won't be abelian.
$r^2 * q * r^2 = r^2 * r^3 * q * r = r * q * r = r * r^3 * q = q$. As required.
3,5,6,7 cannot be orders of subgroups by Lagrange's Theorem.

Isomorphism

Consider the following two groups:
Rotational symmetries of an equilateral triangle:
Addition modulo 3 on $\{0, 1, 2\}$:
They are the same up to the following relabelling of the elements:
$e \to 0, r \to 1, r^2 \to 2$.

Definition

Two groups G_1 and G_2 are said to be **isomorphic** if they have the same structure.
We denote **isomorphism** as $G_1 \cong G_2$.

Showing Isomorphism

Definition

If two groups are isomorphic:

- They must have the same order
- The set of the orders of all the elements must be the same
- The identity of one group will map to the identity of the other

Problem

The group R is defined as $R = (< 4 >, \times_7)$ and the group S as $(\{0, 1, 2\}, +_3)$. Prove that $R \approx S$, fully justifying your answer.

Showing Isomorphism

Definition

If two groups are isomorphic:

- They must have the same order
- The set of the orders of all the elements must be the same
- The identity of one group will map to the identity of the other

Problem

The group R is defined as $R = (< 4 >, \times_7)$ and the group S as $(\{0, 1, 2\}, +_3)$. Prove that $R \approxeq S$, fully justifying your answer.

tables
if we map $1 \to 0, 4 \to 1$ and $2 \to 2$, then this gives us an isomorphism between the two groups.

Test Your Understanding

Problem

The group J is defined as $(\{1, -1, i, -i\}, \times)$ and the group N is defined as $(< 2 >, \times_7)$.
Determine whether the groups J and N are isomorphic, fully justifying your answer.

Problem

Show that the groups shown in the two Cayley tables below are not isomorphic:

Test Your Understanding

Problem

The group J is defined as $(\{1, -1, i, -i\}, \times)$ and the group N is defined as $(< 2 >, \times_7)$.
Determine whether the groups J and N are isomorphic, fully justifying your answer.

$2^1 = 2, 2^2 = 4, 2^3 = 1$.
Therefore the orders of the groups are different, and it is not possible for them to be isomorphic.

Problem

Show that the groups shown in the two Cayley tables below are not isomorphic:

Test Your Understanding

Problem

The group J is defined as $(\{1, -1, i, -i\}, \times)$ and the group N is defined as $(< 2 >, \times_7)$.
Determine whether the groups J and N are isomorphic, fully justifying your answer.

$2^1 = 2, 2^2 = 4, 2^3 = 1$.
Therefore the orders of the groups are different, and it is not possible for them to be isomorphic.

Problem

Show that the groups shown in the two Cayley tables below are not isomorphic:

In the first Cayley table the orders of the elements are 1,2,4 and 4.
In the second all the elements have order 2.
Therefore as the set of orders of the elements is different, the two groups cannot be isomorphic.

Past Paper Question

Problem

The binary operation $*$ is defined as

$$a * b = a + b + 4(\mod 6).$$

Where $a, b \in \mathbb{Z}$.

- *Show that the set $\{0, 1, 2, 3, 4, 5\}$ forms a group G under $*$.*
- *Find the Proper subgroups of the group G.*
- *Determine whether or not the group G is isomorphic to the group $K = (< 3 >, \times_{13}$.*

Past Paper Question

Problem

The binary operation $*$ is defined as

$$a * b = a + b + 4(\mod 6).$$

Where $a, b \in \mathbb{Z}$.

- *Show that the set $\{0, 1, 2, 3, 4, 5\}$ forms a group G under $*$.*
- *Find the Proper subgroups of the group G.*
- *Determine whether or not the group G is isomorphic to the group $K = (< 3 >, \times_{13}$.*

Closure: All answers to $a * b$ are reduced modulo 6 they are in the given set and the set is thus closed under $*$.
Identity: 2
Inverse: (0,4) and (1,3) are inverse pairs, and 2 and 5 are self-inverse elements.
Associativity: Must be shown.
As G satisfies the four group axioms under the binary operation $*$, G is a group.

Past Paper Question

Problem

The binary operation $*$ is defined as

$$a * b = a + b + 4(\mod 6).$$

Where $a, b \in \mathbb{Z}$.

- *Show that the set $\{0, 1, 2, 3, 4, 5\}$ forms a group G under $*$.*
- *Find the Proper subgroups of the group G.*
- *Determine whether or not the group G is isomorphic to the group $K = (< 3 >, \times_{13}$.*

Closure: All answers to $a * b$ are reduced modulo 6 they are in the given set and the set is thus closed under $*$.
Identity: 2
Inverse: (0,4) and (1,3) are inverse pairs, and 2 and 5 are self-inverse elements.
Associativity: Must be shown.
As G satisfies the four group axioms under the binary operation $*$, G is a group.
$\{2\}, \{0, 2, 4\}, \{2, 5\}$.

Past Paper Question

Problem

The binary operation $*$ is defined as

$$a * b = a + b + 4(\mod 6).$$

Where $a, b \in \mathbb{Z}$.

- *Show that the set $\{0, 1, 2, 3, 4, 5\}$ forms a group G under $*$.*
- *Find the Proper subgroups of the group G.*
- *Determine whether or not the group G is isomorphic to the group $K = (< 3 >, \times_{13}$.*

Closure: All answers to $a * b$ are reduced modulo 6 they are in the given set and the set is thus closed under $*$.
Identity: 2
Inverse: (0,4) and (1,3) are inverse pairs, and 2 and 5 are self-inverse elements.
Associativity: Must be shown.
As G satisfies the four group axioms under the binary operation $*$, G is a group.
$\{2\}, \{0, 2, 4\}, \{2, 5\}$.
$G = (< 1 >, *)$, $1 \mapsto 3, 0 \mapsto 9, 5 \mapsto 13, 4 \mapsto 11, 3 \mapsto 5, 2 \mapsto 1$.
As there is a one to one mapping of the elements of G and the elements of K, $G \approxeq K$.