MATH 417, HOMEWORK 12

CHARLES ANCEL

Exercise 5.2.3. Count the number of ways to color the edges of a cube with three colors. Count the number of ways to color the edges of a cube with r colors; the answer is a polynomial in r.

Introduction

In this exercise, we aim to count the number of distinct ways to color the edges of a cube using three different colors. We will employ Burnside's Lemma and Polya's Enumeration Theorem to account for the symmetries of the cube and derive a general formula for r colors.

Solution

Burnside's Lemma: Burnside's Lemma is a tool in group theory for counting the number of orbits of a set X under a group action G. It states that the number of orbits is equal to the average number of fixed points of the elements of G, i.e.,

$$\text{Number of orbits} = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

where X^g is the set of points fixed by g.

Polya's Enumeration Theorem: Polya's Enumeration Theorem is a combinatorial method used to count the number of distinct objects under group actions, taking symmetries into account. It involves using cycle index polynomials to calculate the number of distinct colorings or arrangements.

To count the number of ways to color the edges of a cube with three colors, we will use Burnside's Lemma. The group of rotational symmetries of the cube is isomorphic to the symmetric group S_4, which has 24 elements. Each rotation will fix a certain number of edge colorings.

We will consider the cycle types of these rotations and how many edge colorings they fix.

The cycle index polynomial for the group of rotational symmetries of the cube G is:

$$Z(G) = \frac{1}{|G|} \sum_{g \in G} Z(g)$$

where $Z(g)$ is the cycle type of the permutation induced by g.

The rotational symmetries of the cube and their contributions to the cycle index polynomial are:

1. **Identity rotation (1 element):** Fixes all r^{12} colorings.

$$Z(e) = r^{12}$$

2. **90° and 270° rotations about axes through the centers of faces (6 elements):** Each rotation fixes r^4 colorings (4 cycles of length 3).

$$Z(90^\circ) = Z(270^\circ) = r^4$$

3. **180° rotations about axes through the centers of faces (3 elements):** Each rotation fixes r^6 colorings (6 cycles of length 2).

$$Z(180^\circ) = r^6$$

4. **120° and 240° rotations about axes through the vertices (8 elements):** Each rotation fixes r^3 colorings (3 cycles of length 4).

$$Z(120^\circ) = Z(240^\circ) = r^3$$

5. **180° rotations about axes through the midpoints of edges (6 elements):** Each rotation fixes r^6 colorings (6 cycles of length 2).

$$Z(180^\circ) = r^6$$

Summing these contributions, we get the cycle index polynomial:

$$Z(G) = \frac{1}{24}\left(r^{12} + 6r^4 + 3r^6 + 8r^3 + 6r^6\right) = \frac{1}{24}\left(r^{12} + 6r^4 + 9r^6 + 8r^3\right)$$

To find the number of distinct colorings with 3 colors, we substitute $r = 3$ into the cycle index polynomial:

$$\begin{aligned} Z(G) &= \frac{1}{24}\left(3^{12} + 6 \cdot 3^4 + 9 \cdot 3^6 + 8 \cdot 3^3\right) \\ &= \frac{1}{24}\left(531441 + 6 \cdot 81 + 9 \cdot 729 + 8 \cdot 27\right) \\ &= \frac{1}{24}\left(531441 + 486 + 6561 + 216\right) \\ &= \frac{1}{24}\left(538704\right) = 22446 \end{aligned}$$

Therefore, the number of ways to color the edges of a cube with three colors is 22446.

For r colors, the answer is:

$$Z(G) = \frac{1}{24}\left(r^{12} + 6r^4 + 9r^6 + 8r^3\right)$$

Conclusion

Using Burnside's Lemma and Polya's Enumeration Theorem, we find that the number of distinct ways to color the edges of a cube with three colors is 22446. For r colors, the general formula is given by $Z(G) = \frac{1}{24}(r^{12} + 6r^4 + 9r^6 + 8r^3)$.

Exercise 2. Let G be a finite group. Show that the number of conjugacy classes in G is equal to $\frac{1}{|G|}\sum_{g\in G}|\mathrm{Cent}(g)|$, the average of the orders of the centralizer subgroups.

Introduction

In this exercise, we aim to prove that the number of conjugacy classes in a finite group G is equal to the average of the orders of the centralizer subgroups of the elements of G.

Solution

Centralizer and Conjugacy Classes: The centralizer of an element $g \in G$ is the set $\mathrm{Cent}(g) = \{x \in G \mid xg = gx\}$. The conjugacy class of an element $g \in G$ is the set $\mathrm{CL}(g) = \{xgx^{-1} \mid x \in G\}$. The size of the conjugacy class of g is given by $|\mathrm{CL}(g)| = \frac{|G|}{|\mathrm{Cent}(g)|}$.

Lemma: The number of conjugacy classes of G is the number of distinct conjugacy classes.

Let G be a finite group and let $\mathcal{C}$ be the set of conjugacy classes of G. We want to show that the number of conjugacy classes in G is equal to $\frac{1}{|G|}\sum_{g\in G}|\mathrm{Cent}(g)|$.

Each element $g \in G$ belongs to exactly one conjugacy class, and the size of the conjugacy class of g is given by:

$$|\mathrm{CL}(g)| = \frac{|G|}{|\mathrm{Cent}(g)|}.$$

Summing over all elements $g \in G$, we get:

$$\sum_{g\in G}|\mathrm{CL}(g)| = \sum_{g\in G}\frac{|G|}{|\mathrm{Cent}(g)|}.$$

Since each conjugacy class $\mathrm{CL}(g)$ appears exactly once in this sum, we can rewrite the sum as:

$$\sum_{g\in G}\frac{|G|}{|\mathrm{Cent}(g)|} = |G|\sum_{g\in G}\frac{1}{|\mathrm{Cent}(g)|}.$$

The left-hand side of this equation counts each element of G once for each conjugacy class, giving a total of $|G|$. Therefore, we have:

$$|G| = |G|\sum_{g\in G}\frac{1}{|\mathrm{Cent}(g)|}.$$

Dividing both sides by $|G|$, we get:

$$1 = \sum_{g\in G}\frac{1}{|\mathrm{Cent}(g)|}.$$

To find the number of conjugacy classes, we note that the sum $\sum_{g\in G}|\mathrm{Cent}(g)|$ counts the total number of elements in all centralizers, but each centralizer's size contributes to the

count of its conjugacy class. Therefore:

$$\sum_{g \in G} |\text{Cent}(g)| = \sum_{C \in \mathcal{C}} \sum_{g \in C} |\text{Cent}(g)|.$$

Since $|\text{CL}(g)| = \frac{|G|}{|\text{Cent}(g)|}$, we have $||\text{Cent}(g)| = \frac{|G|}{|\text{CL}(g)|}$. Substituting this in, we get:

$$\sum_{g \in G} |\text{Cent}(g)| = \sum_{C \in \mathcal{C}} |G| = |\mathcal{C}| \cdot |G|.$$

Dividing both sides by $|G|$, we get:

$$\frac{1}{|G|} \sum_{g \in G} |\text{Cent}(g)| = |\mathcal{C}|,$$

which shows that the number of conjugacy classes in G is equal to the average of the orders of the centralizer subgroups.

Conclusion

We have shown that the number of conjugacy classes in a finite group G is equal to the average of the orders of the centralizer subgroups of the elements of G.

Exercise 5.4.1. Suppose $|G| = p^3$, where p is prime. Show that either $|Z(G)| = p$ or G is abelian.

Introduction

In this exercise, we explore the structure of a finite group G of order p^3, where p is a prime number. We aim to show that either the center of the group has order p or the group is abelian.

Solution

Class Equation: The class equation of a group G is given by:

$$|G| = |Z(G)| + \sum_i [G : \text{Cent}(g_i)],$$

where $Z(G)$ is the center of G, and $\text{Cent}(g_i)$ are the centralizers of representatives g_i of the non-central conjugacy classes of G.

Let $|G| = p^3$, where p is prime. According to the class equation, we have:

$$p^3 = |Z(G)| + \sum_i [G : \text{Cent}(g_i)].$$

Note that each term $[G : \text{Cent}(g_i)]$ is the size of a conjugacy class and must divide $|G| = p^3$. Since $|G|$ is a power of a prime, each $[G : \text{Cent}(g_i)]$ must be a power of p. The possible values are 1, p, p^2, and p^3. Since the conjugacy classes that are not singletons contribute at least p elements, $[G : \text{Cent}(g_i)] \geq p$.

Consider the center $Z(G)$. If $Z(G)$ is non-trivial, it must have order p^k where $1 \leq k \leq 3$.

1. **Case 1:** $|Z(G)| = p^3$**:** In this case, $Z(G) = G$, implying that every element commutes with every other element. Hence, G is abelian.

2. **Case 2:** $|Z(G)| = p^2$**:** The class equation becomes:

$$p^3 = p^2 + \sum_i [G : \text{Cent}(g_i)].$$

Simplifying, we get:

$$p^3 - p^2 = p^2(p-1) = \sum_i [G : \text{Cent}(g_i)].$$

This implies there is at least one conjugacy class with $[G : \text{Cent}(g_i)] = p$, and all other classes are singleton. However, this scenario contradicts the class equation since the sum of the indices should match p^2. Thus, $|Z(G)|$ cannot be p^2.

3. **Case 3:** $|Z(G)| = p$**:** The class equation becomes:

$$p^3 = p + \sum_i [G : \text{Cent}(g_i)].$$

Simplifying, we get:

$$p^3 - p = p(p^2-1) = \sum_i [G : \text{Cent}(g_i)].$$

The remaining $p(p^2-1)$ must be distributed among the non-central conjugacy classes. Since each non-central class has size divisible by p, the class sizes could be p, p^2, or both. This scenario is possible, and it implies that G is non-abelian.

Thus, either $|Z(G)| = p$ and G is non-abelian, or $|Z(G)| = p^3$ and G is abelian. Hence, we have shown that either $|Z(G)| = p$ or G is abelian.

Conclusion

We have demonstrated that for a group G of order p^3, where p is prime, either $|Z(G)| = p$ and G is non-abelian, or $|Z(G)| = p^3$ and G is abelian.

Exercise 4. Let N and A be groups, let $\gamma : A \to \mathrm{Aut}(N)$ be a homomorphism, and let $\phi : A \to A$ be an automorphism. Consider the semi-direct product groups:

$$G_1 := N \rtimes_{\gamma\phi} A, \qquad G_2 := N \rtimes_{\gamma} A,$$

where $\gamma\phi = \gamma \circ \phi$ is the composite homomorphism $A \to \mathrm{Aut}(N)$. Show that the function $\omega : G_1 \to G_2$ defined by $(n, a) \mapsto (n, \phi(a))$ is an isomorphism of groups.

Introduction

In this exercise, we explore the relationship between two semi-direct product groups G_1 and G_2 defined by different homomorphisms. We will show that the function $\omega : G_1 \to G_2$ defined by $(n, a) \mapsto (n, \phi(a))$ is an isomorphism of groups.

Solution

Definition: Semi-Direct Product: The semi-direct product $N \rtimes_\gamma A$ of a group N with a group A acting on it via a homomorphism $\gamma : A \to \mathrm{Aut}(N)$ is the group with the underlying set $N \times A$ and multiplication given by:

$$(n_1, a_1) \cdot (n_2, a_2) = (n_1\gamma(a_1)(n_2), a_1a_2).$$

Automorphism: An automorphism $\phi : A \to A$ is a bijective homomorphism from the group A to itself.

Let $G_1 = N \rtimes_{\gamma\phi} A$ and $G_2 = N \rtimes_\gamma A$, and define the function $\omega : G_1 \to G_2$ by $(n, a) \mapsto (n, \phi(a))$. We need to show that ω is an isomorphism of groups.

Step 1: Homomorphism. We show that ω preserves the group operation.

$$\omega((n_1, a_1) \cdot (n_2, a_2)) = \omega((n_1\gamma\phi(a_1)(n_2), a_1a_2)) = (n_1\gamma(\phi(a_1))(n_2), \phi(a_1a_2)).$$

Using the fact that ϕ is a homomorphism, we have:

$$\phi(a_1a_2) = \phi(a_1)\phi(a_2).$$

Thus,

$$\omega((n_1, a_1) \cdot (n_2, a_2)) = (n_1\gamma(\phi(a_1))(n_2), \phi(a_1)\phi(a_2)).$$

On the other hand,

$$\omega(n_1, a_1) \cdot \omega(n_2, a_2) = (n_1, \phi(a_1)) \cdot (n_2, \phi(a_2)) = (n_1\gamma(\phi(a_1))(n_2), \phi(a_1)\phi(a_2)).$$

Hence,

$$\omega((n_1, a_1) \cdot (n_2, a_2)) = \omega(n_1, a_1) \cdot \omega(n_2, a_2).$$

Therefore, ω is a homomorphism.

Step 2: Injectivity. We show that ω is injective. Suppose $\omega(n, a) = \omega(n', a')$. Then,

$$(n, \phi(a)) = (n', \phi(a')).$$

Since ϕ is an automorphism, it is bijective, so $\phi(a) = \phi(a')$ implies $a = a'$. Thus, $n = n'$. Therefore, $(n, a) = (n', a')$ and ω is injective.

Step 3: Surjectivity. We show that ω is surjective. Let $(n, b) \in G_2$. Since ϕ is surjective, there exists an $a \in A$ such that $\phi(a) = b$. Then,

$$\omega(n, a) = (n, \phi(a)) = (n, b).$$

Therefore, ω is surjective.

Since ω is a bijective homomorphism, it is an isomorphism of groups. Hence, the function $\omega : G_1 \to G_2$ defined by $(n, a) \mapsto (n, \phi(a))$ is an isomorphism of groups.

Conclusion

We have shown that the function $\omega : G_1 \to G_2$ defined by $(n, a) \mapsto (n, \phi(a))$ is an isomorphism of groups, demonstrating the relationship between the two semi-direct product groups defined by different homomorphisms.

Exercise 5. This exercise gives a proof of "Fermat's Little Theorem" using the p-group fixed point theorem. Let $G = \langle \phi \rangle$ be a cyclic group of order p, with p-prime, and let $n \in \mathbb{N}$. Define $X = \{(x_1, \ldots, x_p) \mid x_i \in \{1, \ldots, n\}\}$, the set of ordered p-tuples of elements taken from $\{1, \ldots, n\}$. There is an action by G on X defined so that

$$\phi(x_1, x_2, \ldots, x_p) = (x_p, x_1, \ldots, x_{p-1}).$$

Use the p-group fixed point theorem applied to this action to show that $n^p \equiv n \pmod{p}$.

Introduction

In this exercise, we provide a proof of Fermat's Little Theorem using the p-group fixed point theorem. We consider the action of a cyclic group of order p on the set of ordered p-tuples of elements from $\{1, \ldots, n\}$ and apply the fixed point theorem to derive the theorem.

Solution

Fermat's Little Theorem: Fermat's Little Theorem states that if p is a prime number and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$. Equivalently, $a^p \equiv a \pmod{p}$.

p-Group Fixed Point Theorem: If a p-group G acts on a finite set X, then the number of fixed points of the action is congruent to the size of X modulo p. In other words, $|\mathrm{Fix}(G, X)| \equiv |X| \pmod{p}$.

Let $G = \langle \phi \rangle$ be a cyclic group of order p, and consider the set $X = \{(x_1, \ldots, x_p) \mid x_i \in \{1, \ldots, n\}\}$. The group G acts on X by cyclically permuting the coordinates:

$$\phi(x_1, x_2, \ldots, x_p) = (x_p, x_1, \ldots, x_{p-1}).$$

The total number of elements in X is n^p since there are n choices for each of the p coordinates. We need to count the number of fixed points of the action of ϕ on X.

An element $(x_1, x_2, \ldots, x_p) \in X$ is fixed by ϕ if:

$$\phi(x_1, x_2, \ldots, x_p) = (x_1, x_2, \ldots, x_p).$$

This implies:

$$(x_p, x_1, \ldots, x_{p-1}) = (x_1, x_2, \ldots, x_p).$$

Thus, $x_1 = x_2 = \cdots = x_p$. Each coordinate must be the same, so there are n fixed points, corresponding to the n possible values for x_1.

By the p-group fixed point theorem, the number of fixed points is congruent to the size of the set X modulo p:

$$|\mathrm{Fix}(G, X)| \equiv |X| \pmod{p}.$$

Substituting the values, we get:

$$n \equiv n^p \pmod{p}.$$

Hence, $n^p \equiv n \pmod{p}$, which completes the proof using the p-group fixed point theorem.

Conclusion

We have used the p-group fixed point theorem to prove Fermat's Little Theorem, showing that $n^p \equiv n \pmod{p}$ for any integer n and prime p.

Exercise 6. Let $Q := \{\pm I, \pm A, \pm B, \pm C\} \subseteq \mathrm{GL}_2(\mathbb{C})$, where

$$A := \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \qquad B := \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \qquad C := AB = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

Verify the formulas

$$A^2 = B^2 = C^2 = -I \qquad AB = C,\ BC = A,\ CA = B \qquad BA = -C,\ CB = -A,\ AC = -B$$

and conclude that Q is a subgroup of $\mathrm{GL}_2(\mathbb{C})$ of order 8. What are the orders of the elements of Q? What are the conjugacy classes in Q? Show that Q is not isomorphic to D_4.

Introduction

In this exercise, we investigate a subset Q of the general linear group $\mathrm{GL}_2(\mathbb{C})$ and verify specific algebraic properties. We aim to show that Q forms a subgroup of order 8, determine the orders of its elements and its conjugacy classes, and demonstrate that Q is not isomorphic to the dihedral group D_4.

Solution

Verification of Formulas:

Verify $A^2 = -I$:

$$A^2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = -I.$$

Verify $B^2 = -I$:

$$B^2 = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} i^2 & 0 \\ 0 & (-i)^2 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = -I.$$

Verify $C^2 = -I$:

$$C^2 = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} = \begin{bmatrix} -i^2 & 0 \\ 0 & -i^2 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = -I.$$

Verify $AB = C$:

$$AB = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} = C.$$

Verify $BC = A$:

$$BC = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = A.$$

Verify $CA = B$:

$$CA = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = B.$$

Verify $BA = -C$:

$$BA = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix} = -\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} = -C.$$

Verify $CB = -A$:

$$CB = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = - \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = -A.$$

Verify $AC = -B$:

$$AC = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} = \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix} = - \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = -B.$$

Conclusion: We have verified the given formulas. Hence, $Q = \{\pm I, \pm A, \pm B, \pm C\}$ is a subgroup of $\mathrm{GL}_2(\mathbb{C})$ of order 8.

Orders of the Elements of Q:

- $\pm I$: Order 1.
- $\pm A$, $\pm B$, $\pm C$: Order 4 (since $A^2 = B^2 = C^2 = -I$, and $(-I)^2 = I$).

Conjugacy Classes in Q: To find the conjugacy classes, we note that Q is generated by I, A, B, C, and their negatives.

- $\{I\}$: Conjugacy class of I.
- $\{-I\}$: Conjugacy class of $-I$.
- $\{A, -A\}$: Conjugacy class of A and $-A$.
- $\{B, -B\}$: Conjugacy class of B and $-B$.
- $\{C, -C\}$: Conjugacy class of C and $-C$.

Non-Isomorphism to D_4: D_4 has elements of orders 1, 2, and 4. Since Q has elements of orders 1 and 4 only, it cannot be isomorphic to D_4.

Hence, Q is not isomorphic to D_4.

Conclusion

We have shown that the set Q is a subgroup of $\mathrm{GL}_2(\mathbb{C})$ of order 8, verified the algebraic properties of its elements, determined its conjugacy classes, and demonstrated that it is not isomorphic to the dihedral group D_4.

Exercise 7. Let S be the subset of the ring $M := \mathrm{Mat}_{2\times 2}(\mathbb{R})$ consisting of matrices of the form $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$. Show that S is a subring of M. Determine whether S is a commutative ring, and whether S has a multiplicative identity element.

Introduction

In this exercise, we examine a subset S of the ring of 2×2 matrices over $\mathbb{R}$. We aim to show that S forms a subring of M, determine its commutativity, and check for the existence of a multiplicative identity element.

Solution

Definition of Subring: A subset S of a ring M is a subring if it is closed under addition, subtraction, and multiplication, and contains the multiplicative identity of M.

Step 1: Closure under Addition. Let $A = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ and $B = \begin{bmatrix} a' & b' \\ 0 & d' \end{bmatrix}$ be elements of S. Then,

$$A + B = \begin{bmatrix} a + a' & b + b' \\ 0 & d + d' \end{bmatrix}.$$

Since $a + a'$, $b + b'$, and $d + d'$ are real numbers, $A + B \in S$.

Step 2: Closure under Subtraction. Similarly,

$$A - B = \begin{bmatrix} a - a' & b - b' \\ 0 & d - d' \end{bmatrix}.$$

Since $a - a'$, $b - b'$, and $d - d'$ are real numbers, $A - B \in S$.

Step 3: Closure under Multiplication.

$$AB = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \begin{bmatrix} a' & b' \\ 0 & d' \end{bmatrix} = \begin{bmatrix} aa' & ab' + bd' \\ 0 & dd' \end{bmatrix}.$$

Since aa', $ab' + bd'$, and dd' are real numbers, $AB \in S$.

Step 4: Containing the Multiplicative Identity. The multiplicative identity in $\mathrm{Mat}_{2\times 2}(\mathbb{R})$ is $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, which is of the form $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ with $a = 1$, $b = 0$, and $d = 1$. Therefore, $I \in S$.

Thus, S is a subring of M.

Step 5: Commutativity.

$$AB = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \begin{bmatrix} a' & b' \\ 0 & d \end{bmatrix} = \begin{bmatrix} aa' & ab' + bd' \\ 0 & dd' \end{bmatrix}.$$

$$BA = \begin{bmatrix} a' & b' \\ 0 & d' \end{bmatrix} \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} = \begin{bmatrix} a'a & a'b + b'd \\ 0 & d'd \end{bmatrix}.$$

Since $ab' + bd' \neq a'b + b'd$ in general, S is not a commutative ring.

Step 6: Multiplicative Identity. The matrix $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ serves as the multiplicative identity in S.

Therefore, S has a multiplicative identity element but is not commutative.

Conclusion

We have shown that the subset S of matrices of the form $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ forms a subring of $M := \mathrm{Mat}_{2\times 2}(\mathbb{R})$, contains the multiplicative identity, but is not commutative.

Exercise 8. Do the same with the subset S' of $M := \mathrm{Mat}_{2\times 2}(\mathbb{R})$ consisting of matrices of the form $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$.

Introduction

In this exercise, we examine a subset S' of the ring of 2×2 matrices over $\mathbb{R}$. We aim to show that S' forms a subring of M, determine its commutativity, and check for the existence of a multiplicative identity element.

Solution

Definition of Subring: A subset S' of a ring M is a subring if it is closed under addition, subtraction, and multiplication, and contains the multiplicative identity of M.

Step 1: Closure under Addition. Let $A = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} a' & 0 \\ 0 & 0 \end{bmatrix}$ be elements of S'. Then,

$$A + B = \begin{bmatrix} a + a' & 0 \\ 0 & 0 \end{bmatrix}.$$

Since $a + a'$ is a real number, $A + B \in S'$.

Step 2: Closure under Subtraction. Similarly,

$$A - B = \begin{bmatrix} a - a' & 0 \\ 0 & 0 \end{bmatrix}.$$

Since $a - a'$ is a real number, $A - B \in S'$.

Step 3: Closure under Multiplication.

$$AB = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a' & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} aa' & 0 \\ 0 & 0 \end{bmatrix}.$$

Since aa' is a real number, $AB \in S'$.

Step 4: Containing the Multiplicative Identity. The multiplicative identity in $\mathrm{Mat}_{2\times 2}(\mathbb{R})$ is $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, which is not of the form $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$. Therefore, S' does not contain the multiplicative identity of M.

Thus, S' is a subring of M.

Step 5: Commutativity.

$$AB = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a' & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} aa' & 0 \\ 0 & 0 \end{bmatrix}.$$

$$BA = \begin{bmatrix} a' & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a'a & 0 \\ 0 & 0 \end{bmatrix}.$$

Since $aa' = a'a$, S' is a commutative ring.

Step 6: Multiplicative Identity. There is no multiplicative identity in S' because the form $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ does not act as a multiplicative identity for all elements of S'.

Therefore, S' is a commutative subring of M but does not have a multiplicative identity element.

Conclusion

We have shown that the subset S' of matrices of the form $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$ forms a subring of $M := \mathrm{Mat}_{2\times 2}(\mathbb{R})$, is commutative, but does not contain a multiplicative identity.