TOPIC 1: ALGEBRA

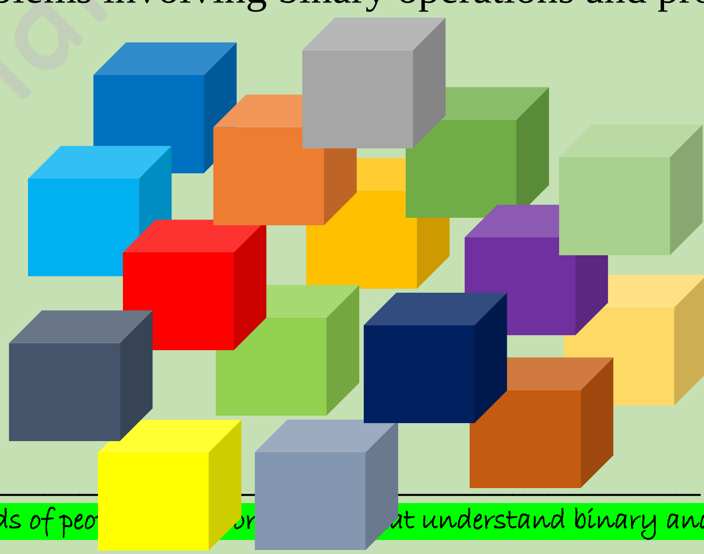
Prepared by G. Manuwere

1.2 GROUPS

Learning Objectives

After completing this topic you should be able to:

- define a binary operation
- define closure, commutation, association, distribution, identity and inverse element
- define a group
- use the basic properties to show that a given structure is, or is not, a group
- solve problems involving binary operations and properties of a group



"There are 10 kinds of peo[illegible] or [illegible] at understand binary and the other 9" Jonathan Kariv

gmanuwere@gmail.com /+263773975592/+263737967477

1.2.1 Binary operations

- Binary means composed of two parts.
- A binary is a rule for combining two values to create a new value.
- Binary operation on a set is a calculation involving two elements of a set to produce another element of the set.
- A binary operation on set S is a function $*$ such that $a * b = y$ where a, b and y are elements of set S.
- The notation $(S,*)$ can be used to indicate that set S has a binary operation $*$.
- The symbol $*$ can be used to represent a law of binary composition.
- Basic binary operations are $\times;\ \div;\ +;\ -$.
- A binary operation on a finite set can be displayed on a Cayley table or Latin square which shows how operations are to be performed.

Properties of binary operation

(a) Closure

The set S is closed under a binary operation $*$ if, for every pair of elements a and b of set S, $a * b$ is also an element of set S.

The binary operation $*$ is said to be a closed binary operation on set S.

Example 1

Determine whether the following set is closed under the given law of binary operation.

(i) Integers, multiplication.

(ii) Natural numbers, subtraction.

Solution

(i) The set of integers is given by $\mathbb{Z} = \{\ldots -3; -2; -1; 0; 1; 2; 3; \ldots\}$

$(\mathbb{Z}; \text{x})$

It is clear that $\forall a, b \in \mathbb{Z}$, $a\text{x}b \in \mathbb{Z}$. E.g. if $a = -3$ $b = 4$, $-3\text{x}4 = -12 \in \mathbb{Z}$. Hence the set of integers is closed under multiplication.

"There are 10 kinds of people in the world, those that understand binary and the other 9" Jonathan Kariv

(ii) The set of natural numbers is given by $\mathbb{N} = \{1; 2; 3; \dots\}$

$(\mathbb{N}; -)$

We will use a counter example to determine this.
let $a, b \in \mathbb{N}$ where $a = 2$ and $b = 3$.

$2 - 3 = -1 \notin \mathbb{N}$.

Hence the set of natural numbers is not closed under subtraction.

Example 2

Determine whether the binary operation $*$ of multiplication is closed on set G, where $G = \{-1; 1; -i; i\}$ is a set of complex numbers of unit moduli.

Solution

Set G is a finite set and so we can use the following operation table to show all the possible outcomes.

x	-1	1	$-i$	i
-1	1	-1	i	$-i$
1	-1	1	$-i$	i
$-i$	i	$-i$	-1	1
i	$-i$	i	1	-1

Every element in the table is a member of the set G. Hence the binary operation $*$ is closed.

(b) Commutativity

A binary operation $*$ on a set S is said to be commutative if for all $a, b \in S$, the equality $a * b = b * a$ holds, ie, the order of the pair does not affect the result.

"There are 10 kinds of people in the world, those that understand binary and the other 9" Jonathan Kariv

Example 1

(i) Show that multiplication is commutative on the set $\mathbb{Z}$ of integers.

(ii) The operation $\circ$ on real numbers is defined by $a \circ \mathrm{b} = a|b|$.

Show that $\circ$ is not commutative.

(iii) A set $M = \{a, b, c, d\}$ under a binary operation $*$ has an operation table as follows:

$*$	a	b	c	d
a	c	d	a	b
b	d	c	b	a
c	a	b	c	d
d	b	a	d	c

Show that $*$ is commutative on the set M.

Solution

(i) $\mathbb{Z} = \{\ldots -2, -1, 0, 1, 2, \ldots\}$

$(\mathbb{Z}; \mathrm{x})$

It is clear that $\forall a, b \in \mathbb{Z}\ a \text{ x } b = b \text{ x } a$. Eg if $a = -2$ and $b = 7$

$-2 \text{ x } 7 = 7 \text{ x } -2 = -14$.

Hence multiplication is commutative on the set $\mathbb{Z}$ of positive integers.

(ii) $a \circ \mathrm{b} = a|b|\ \forall a, b \in \mathbb{R}$

For commutativity, $a \circ \mathrm{b} = b \circ a$

LHS $a \circ \mathrm{b} = a|b|$ RHS $b \circ a = b|a|$

$a|b| \neq b|a|$ hence $\circ$ is not commutative.

"There are 10 kinds of people in the world, those that understand binary and the other 9" Jonathan Kariv

(iii)

$*$	a	b	c	d
a	c	d	a	b
b	d	c	b	a
c	a	b	c	d
d	b	a	d	c

The table is symmetrical about the main diagonal (as shown by the red line) hence $*$ is commutative on M.

(c) Associativity

The binary operation $*$ on a set S is said to be associative if for for every three elements $a, b, c \in S$ then $a * (b * c) = (a * b) * c$.

Example 1

The operation $\circ$ on real numbers is defined by $a \circ \mathrm{b} = a|b|$.

Determine whether $\circ$ is associative.

Solution

$a \circ \mathrm{b} = a|b|\ \forall a, b \in \mathbb{R}$

Let $a, b, c \in \mathbb{R}$.

We want to show that $a \circ (b \circ c) = (a \circ b) \circ c$

LHS $a \circ (b \circ \mathrm{c}) = a \circ (\mathrm{b}|\mathrm{c}|) = a\big|b|c|\big| = a|bc|$

RHS $(a \circ \mathrm{b}) \circ \mathrm{c} = (a|b|) \circ \mathrm{c} = a|b||c| = a|bc|$

LHS = RHS hence $\circ$ is associative.

"There are 10 kinds of people in the world, those that understand binary and the other 9" Jonathan Kariv

Example 2

Given that $*$ is a binary operation on the set $\mathbb{Z}$, of integers defined by

$a * b = a + b + ab$

(i) Evaluate $3 * 4$

(ii) Prove that $*$ is both commutative and associative and $\mathbb{Z}$.

Solution

(i) $3 * 4 = 3 + 4 + 3(4) = 19$

(ii) Commutativity: to prove that $a * b = b * a \ \forall a, b \in \mathbb{Z}$

LHS $\Longrightarrow a * b = a + b + ab$

RHS $\Longrightarrow b * a = b + a + ba$

$= a + b + ab.$

LHS=RHS Hence $*$ is commutative

Associativity: to prove that $\forall a, b, c \in \mathbb{Z}, a * (b * c) = (a * b) * c$

Now, $b * c = b + c + bc$

LHS $\Longrightarrow a * (b * c) = a * (b + c + bc) = a + b + c + bc + ab + ac + abc$

Also,

RHS$\Longrightarrow (a * b) * c = (a + b + ab) * c = a + b + ab + c + ac + bc + abc$

$= a + b + c + bc + ab + ac + abc$

LHS=RHS Hence $*$ is associative

"There are 10 kinds of people in the world, those that understand binary and the other 9" Jonathan Kariv

(d) Identity element (Neutral element)

Given a set S defined on a binary operation $*$, the identity element (if it exists) is a neutral element e in S such that for all $a \in S$, $a * e = e * a = a$.

The identity element, if it exists, is unique. That is to say, the set S has only one identity element.

The identity element when multiplying real numbers is 1.

For any real number a,

$1\text{x}a = a\text{x}1 = a$

The identity element when multiplying 2x2 matrices is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

For any 2x2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$,

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

Zero (0) is the identity element when adding real numbers.

For any real number a,

$0 + a = a + 0 = a$

Example 1

The binary operation $*$ is defined on set $\mathbb{R}$ by $m * n = m + n + 6$ for all $m, n \in \mathbb{R}$. Find the identity element of $\mathbb{R}$ under the binary operation $*$.

Solution

$m * n = m + n + 6 \;\forall\; m, n \in \mathbb{R}.$

"There are 10 kinds of people in the world, those that understand binary and the other 9" Jonathan Kariv

We want to find an element $e \in \mathbb{R}$, which satisfies $m * e = e * m = m$.

Taking the equation $m * e = m$

$$\Longrightarrow m + e + 6 = m$$

$$\Longrightarrow e = m - m - 6$$

$$\Longrightarrow e = -6$$

Thus the identity element is -6.

Example 2

The binary operation $*$ is defined on set M of positive numbers is given $a * b = \frac{a+b}{3ab}$, for all $a, b \in M$. Find, if it exists, the identity element of M under the binary operation $*$.

Solution

$a * b = \frac{a+b}{3ab}$ for all $a, b \in M$

Looking for an element e of M which satisfies $e * a = a * e = a$

Taking the equation $e * a = a$

$$\Longrightarrow \frac{e+a}{3ea} = a$$

$$\Longrightarrow e + a = 3ea^2$$

$$\Longrightarrow 3ea^2 - e = a$$

$$\Longrightarrow e(3a^2 - 1) = a$$

$$\Longrightarrow e = \frac{a}{3a^2-1}$$

$\frac{a}{3a^2-1}$ can not be an identity element since the identity is a unique element.

Thus M does not have an identity element.

“There are 10 kinds of people in the world, those that understand binary and the other 9” Jonathan Kariv

Example 3

The binary operation $*$ is defined on set $\mathbb{R}$ by $p * q = p + q - 4p^2q^2$ for all $p, q \in \mathbb{R}$. Find the identity element of $\mathbb{R}$ under the binary operation $*$.

Solution

Looking for an element e of $\mathbb{R}$ which satisfies $e * a = a * e = a$ for all $a \in \mathbb{R}$

Taking $a * e = a$

$\Longrightarrow a + e - 4a^2e^2 = a$

$\Longrightarrow e - 4a^2e^2 = 0$

$\Longrightarrow e(1 - 4a^2e) = 0$

$\Longrightarrow e = 0$ or $\frac{1}{4a^2}$

The identity element is unique if it exists. $e = 0$ is the identity element under $*$.

Example 4

The binary operation $*$ is defined on the set R of ordered pairs of real numbers by $(x, y) * (p, q) = (x + p, yq)$ for all $x, y, p, q \in \mathbb{R}$.

(a) Show that

(i) R is commutative under the binary operation $*$.

(ii) R is associative under the binary operation $*$.

(b) Find the identity element of R under the binary operation $*$.

Solution

(a) (i) Let $x, y, p, q \in \mathbb{R}$

For commutativity we want to prove that $(x, y) * (p, q) = (p, q) * (x, y)$

LHS $(x, y) * (p, q) = (x + p, yq)$

"There are 10 kinds of people in the world, those that understand binary and the other 9" Jonathan Kariv

RHS $(p,q)*(x,y)=(p+x,qy)=(x+p,yq)$

LHS = RHS hence R is commutative under the binary operation $*$..

(ii) Let $x,y,p,q,m,n\in\mathbb{R}$

For associativity we want to prove that
$(x,y)*[(p,q)*(m,n)]=[(x,y)*(p,q)]*(m,n)$

Now $(p,q)*(m,n)=(p+m,qn)$

$\therefore$ LHS $(x,y)*[(p,q)*(m,n)]=(x,y)*(p+m,qn)$

$=(x+p+m,yqn)$

RHS $[(x,y)*(p,q)]*(m,n)=(x+p,yq)*(m,n)$

$=(x+p+m,yqn)$

LHS = RHS hence R is associative with respect to the binary operation $*$.

(b) Let $x,y,a,b\in\mathbb{R}$

We want to find an identity element (a,b) such that

$(x,y)*(a,b)=(a,b)*(x,y)=(x,y)$

Taking the equation $(x,y)*(a,b)=(x,y)$

$\Longrightarrow (x+a,yb)=(x,y)$

Thus $x+a=x$ and $yb=y$

$\Longrightarrow a=0$ and $y=y$

Hence the identity element is $(0,y)$

(e) Inverse Element

Given a set S defined under a binary operation $*$. For each element a in S, there exists a unique inverse for each element, a^{-1}, which is such that $a*a^{-1}=a^{-1}*a=e$ where $a^{-1},e\in S$. e is the identity element.

"There are 10 kinds of people in the world, those that understand binary and the other 9" Jonathan Kariv

The inverse of an element, if it exists, under given binary operation is unique for each element.

Example 1

A binary operation $*$ is defined on the set of real numbers, $\mathbb{R}$, by $m * n = m + n + 2mn$, for all $m, n \in \mathbb{R}$. Find

(i) the identity element e of $\mathbb{R}$ under $*$.

(ii) the inverse x^{-1} of x, where $x \in \mathbb{R}$.

(iii) for what value of x is x^{-1} not defined?

Solution

(i) Looking for an $e \in \mathbb{R}$ such that $m * e = e * m = m$ for all $m \in \mathbb{R}$

Taking the equation $m * e = m$

$$\Longrightarrow m + e + 2me = m$$

$$\Longrightarrow e(1 + 2m) = 0$$

$$\Longrightarrow e = 0$$

(ii) x^{-1}, the inverse of x satisfies $x * x^{-1} = x^{-1} * x = e$ where $e = 0$.

Taking the equation $x * x^{-1} = 0$

$$\Longrightarrow x + x^{-1} + 2xx^{-1} = 0$$

$$\Longrightarrow x^{-1} + 2xx^{-1} = -x$$

$$\Longrightarrow x^{-1}(1 + 2x) = -x$$

$$\Longrightarrow x^{-1} = \frac{-x}{1+2x}$$

(iii) x^{-1} is undefined when the denominator is zero that is when $x = -\frac{1}{2}$.

Example 2

The binary operation $*$ is defined on the set $\mathbb{R}$ of real numbers by $m * n = m + n + 3$, for all $m, n \in \mathbb{R}$.

(i) Find the inverse of a under the binary operation $*$ of real numbers.

(ii) Find the inverse of 4.

Solution

(i) We first find the identity element e under $*$

Let $m, e \in \mathbb{R}$.

$m * e = e * m = m$

Taking $m * e = m$

$\Longrightarrow m + e + 3 = m$

$\Longrightarrow e = -3$

We now find a real number a^{-1}such that $a * a^{-1} = a^{-1} * a = -3$

Taking $a^{-1} * a = 3$

$\Longrightarrow a^{-1} + a + 3 = -3$

$\Longrightarrow a^{-1} = -a - 6$

(ii) $4^{-1} = -4 - 6 = -10$

Modular Arithmetic

Modular arithmetic is a system of arithmetic for integers, which considers the remainder after dividing two integers.

In general:

If $a \div n = q + R$ where q is the quotient and R is the remainder, we say that $a \text{ mod } n = R$ where $0 \leq R < n$. The focus is on the remainder after dividing a by n.

For instance $18 mod 5 = 3$, $21 mod 4 = 1$ and $16 mod 4 = 0$

"There are 10 kinds of people in the world, those that understand binary and the other 9" Jonathan Kariv

Example 3

The set $G = \{0; 1; 2; 3; 4; 5\}$, is defined under the binary operation $*$ of addition (mod 6). Complete a Cayley table for the operation. State the identity element for set and the inverse for each element. Determine whether $*$ is associative.

Solution

$+_6$	**0**	**1**	**2**	**3**	**4**	**5**
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Clearly, the identity element is 0.

Element	0	1	2	3	4	5
Inverse	0	5	4	3	2	1

For associativity, consider any three elements, 0, 1 and 2 say.

$0 * (1 * 2) = (0 * 1) * 2 = 3$ Hence in general, $*$ is associative.

"There are 10 kinds of people in the world, those that understand binary and the other 9" Jonathan Kariv

Example 4

The table below defines the binary operation $*$ on the set M, where $M = \{a, b, c, d\}$.

(a) Find, giving reasons, whether or not

(i) M is closed with respect to $*$.

(ii) the operation $*$ is commutative.

(iii) There is an identity element.

(b) Find, where possible, the inverse of each element a, b, c and d.

$*$	a	b	c	d
a	b	d	a	c
b	d	c	b	a
c	a	b	c	d
d	c	a	d	b

Solution

(a) (i) M is closed under $*$ because all outcomes in the table are elements of set M.
(ii) The table is symmetrical about the main diagonal, hence $*$ is commutative.
(ii) c is the identity element because for each element x in M, $x * c = c * x = x$.
(b)

Element	a	b	c	d
Inverse	d	b	c	a

(f) Distributive

The distributive property uses two binary operations on the same set.
If the binary operations $*$ and $\otimes$ are defined on the set S such that;

$a * (b \otimes c) = (a * b) \otimes (a * c)$.

"There are 10 kinds of people in the world, those that understand binary and the other 9" Jonathan Kariv

Then the operation $*$ is said to be distributive over the operation $\otimes$.

The distributive property is simple. It is just a matter of one operation having authority over another operation.
If an operation overrules another operation, we say the overruling operation is distributive over the other.

Example 1

The binary operations of addition " + " and multiplication "x" are defined on the set $\mathbb{R}$.

Determine whether or not

(a) "x" is distributive over " + ",

(b) " + " is distributive over "x".

Solution

(a) If $a, b, c \in \mathbb{R}$ $\quad a \text{ x}(b + c) = (a \text{ x } b) + (a \text{ x } c)$, hence "x" is distributive over " + ".

(b) If $a, b, c \in \mathbb{R}$ $\quad a$ +(b x c)$\neq$ $(a + b)\text{x}(a + c)$, hence "+" is not distributive over "x".

Example 2

The binary operations $*$ and $\otimes$ are defined on the set $\mathbb{R}$ by $x * y = x^2 - y^2$ and $x \otimes y = x + 2y$, for all $x, y \in \mathbb{R}$.

(a) Evaluate (i) $1 * (2 \otimes 3)$ (ii) $(1 * 2) \otimes (1 * 3)$

(b) Comment on your results for part (i) and (ii)?

Solution

(a) (i) $1 * (2 \otimes 3)$

$2 \otimes 3 = 2 + 2(3) = 8$

$\therefore 1 * (2 \otimes 3) = 1 * 8 = 1^2 - 8^2 = -63$

"There are 10 kinds of people in the world, those that understand binary and the other 9" Jonathan Kariv

(ii) $(1*2)\otimes(1*3) = (1^2 - 2^2)\otimes(1^2 - 3^2)$

$= -3 \otimes -8$

$= -3 + 2(-8)$

$= -19$

(b) $1*(2\otimes 3) \neq (1*2)\otimes(1*3)$ hence $*$ is not distributive over $\otimes$.

Exercise 1.2.1

1 Determine whether the binary operation on $\mathbb{R}$ defined by $a * b = a + b$ is closed, associative and commutative. Find the identity element and the inverse of each element.

2 Find out whether the binary operation on the set of rational numbers $\mathbb{Q}$ defined by $a * b = \frac{a}{b}$ is closed, associative or commutative.

3 Prove that the operation $*$ defined by $a * b = a^b$ on the set $\mathbb{N}$ is not associative or commutative. You may use counterexamples.

4 Prove that the binary operation on $\mathbb{R}$ defined by $a * b = a + b - 1$ is both associative and commutative.

5 Show that the binary operation on $\mathbb{R}$ defined by $a * b = 1 + ab$ is commutative but not associative.

6 Find the identity element of the operation $a * b = a + b - 1$ on the set of integers, $\mathbb{Z}$.

7 Show that the operation $a * b = 1 + ab$ on the set of integers $\mathbb{Z}$ has no identity element.

8 Consider the operation $*$ on the set of integers defined by $a * b = a + b - 1$. Show that each integer has an inverse under this operation.

9 If $*$is defined on $\mathbb{Z}$ by $x * y = x + y + 1$. Find the identity element and the inverse of each element.

10 The operation $*$ is defined on the elements (a, b), where $a, b \in \mathbb{R}$ by

$$(a, b) * (c, d) = (ac, ad + b).$$

It is given that the identity element is $(1,0)$.

(a) Prove that $*$ is associative.

(b) Find all the elements which commute with $(1,1)$.

gmanuwere@gmail.com /+263773975592/+263737967477

(c) It is given that the particular element (m,n) has an inverse denoted by (p,q), where $(m,n) * (p,q) = (p,q) * (m,n) = (1,0)$

Find (p,q) in terms of m and n.

(d) Find all self-inverse elements.

11 (a) The operation $*$ is defined by $x * y = x + y - a$, where x and y are real numbers and a is a real constant.

(i) Prove that the set of real numbers under the operation $*$ is closed and associative.

(ii) Find the identity and inverse element.

(iii) Determine whether the set of real numbers is commutative under the given binary operation.

(b) The binary operation $\circ$ given by $x \circ y = x + y - 5$ is defined over a set of **positive** real numbers. Show, by giving a counterexample or otherwise, that the properties of closure and inverse are not satisfied.

1.2.2 Groups

A group $(G;*)$ is a non-empty set G with binary operation $*$ satisfying the following basic properties(axioms):

(i) Closure – For every pair of elements a and b in set G then $a * b \in G$.

(ii) Associativity-For any three elements a, b and c in G, the equality $a * (b * c) = (a * b) * c$ must hold.

"There are 10 kinds of people in the world, those that understand binary and the other 9" Jonathan Kariv

(iii) Identity element-There is a group element e in G, the identity element, such that $e * a = a * e = a$ for all $a \in G$.

(iv) Inverse - Every element a in G has an inverse, a^{-1}, such that $a * a^{-1} = a^{-1} * a = e$ where a, a^{-1} and e are elements of set G.

Abelian group

A group (G;$*$) which satisfies the commutative property is called an **Abelian group**.
The commutative property says $\forall a, b \in G$ then $a * b = b * a$.
Check for commutative in order to determine whether the given structure is an Abelian group or not. All basic properties of a group are still valid.

Subgroup

A subset H of a group G is a subgroup of G if H is itself a group under the operation in G.

Note: Every group G has at least two subgroups: G itself and the subgroup $\{e\}$, containing only the identity element. All other subgroups are said to be **proper** subgroups.

Definition. Let $(G; *)$ be a group. A subset H of G is called a subgroup if it satisfies the following conditions:

(i) $e \in H$

(ii) H is closed under $*$, that is if $x, y \in H$, then $x * y \in H$

(iii) H is closed under inversion, that is if $\in H$, then $x^{-1} \in$ H

Example 1

The composition table for a group G of order 8 is given below

	a	b	c	d	e	f	g	h
a	c	e	b	f	a	h	d	g
b	e	c	a	g	b	d	h	f
c	b	a	e	h	c	g	f	d
d	f	g	h	a	d	c	e	b
e	a	b	c	d	e	f	g	h
f	h	d	g	c	f	b	a	e
g	d	h	f	e	g	a	b	c
h	g	f	d	b	h	e	c	a

State which is the identity element and give the inverse of each element of G.

Solution

The identity element is e.

Element	a	b	c	d	e	f	g	h
Inverse	b	a	c	g	e	h	d	f

Example 2

Show that the set $\{5, 15, 25, 35\}$ is a group under multiplication modulo 40.

Solution

	5	15	25	35
5	25	35	5	15
15	35	25	15	5
25	5	15	25	35
35	15	5	35	25

"There are 10 kinds of people in the world, those that understand binary and the other 9" Jonathan Kariv

Closure

All elements in the table are members of the set $\{5, 15, 25, 35\}$, hence the set is closed under multiplication modulo 40.

Associativity

Since we have $a(bc) = a(bc)$ for every a, b, c in $\mathbb{Z}$, we get $a(bc) = (ab)c$ for every a, b, c in $\{5, 15, 25, 35\}$. Hence associativity is satisfied.

Identity

25 is the identity element. Observe that $25 \cdot a = a \cdot 25 = a$ for all a in $\{5, 15, 25, 35\}$.

Inverse

Each element is its own inverse.

Since the set $\{5, 15, 25, 35\}$ with multiplication modulo 40 satisfies all requirements given in the definition of a group, $\{5, 15, 25, 35\}$ is a group under the multiplication modulo 40.

Example 3

(a) Show that the set $S = \{0, 1, 2, 3\}$ forms a group under addition (mod 4).

(b) Show that the set S in (a) is an Abelian group.

(c) State all subgroups of S.

Solution

(a)

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Line of symmetry

Closure

All outcomes in the table are members of the set S, hence S is closed under addition (mod4).

Associativity

The set S is associative since for any three elements $a, b, c \in S$, $a + (b + c) = (a + b) + c$

Identity

0 is the identity element

Inverse

Every element has an inverse

Element	0	1	2	3
Inverse	0	3	2	1

Since the set S satisfies all the 4 group axioms, set S forms a group under addition (mod4).

(b) The table is symmetrical about the main diagonal hence the set S is commutative under addition (mod 4). Thus set S is an Abelian group.

(c) Subgroups are $\{0\}$, $\{0,1,2,3\}$, $\{0, 2\}$.

Notice that the sets $\{0, 1\}$, $\{0, 3\}$, $\{0, 1, 2\}$,$\{0, 2, 3\}$ *and* $\{0, 1, 3\}$ *and cannot be subgroups of S because each of these sets violet either closure or inverse property.*

Example 4

Let G be the set of all 3x3 real matrices of the form $\begin{bmatrix} 1 & p & q \\ 0 & 1 & r \\ 0 & 0 & 1 \end{bmatrix}$ where $p, q, r \in \mathbb{R}$. Prove that G forms a group under matrix multiplication.

Solution

Closure

Let $a, b, c, d, e, f \in \mathbb{R}$. Then $\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+d & e+af+b \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{bmatrix} \in G$

Hence the set G is closed under matrix multiplication.

Associativity

For any three matrices A, B and C in G, $(AB)C = A(BC)$ (matrix multiplication is associative).

Identity

The identity 3 x 3 matrix is $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ which is an element of G.

Inverse

For all $A \epsilon G$ such that $A = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$, $A^{-1} = \begin{bmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix} \in G$

Thus every element has an inverse

Since G satisfies all the properties of a group, G forms a group under matrix multiplication.

"There are 10 kinds of people in the world, those that understand binary and the other 9" Jonathan Kariv

Example 4

Let H be the set of all matrices of the form $\begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix}$, where $y \in \mathbb{R}$.

Show that

(i) H does not form a group under matrix addition.

(ii) H forms an abelian group under matrix multiplication. [Assume associativity]

(Zimsec Specimen paper 2018)

Solution

Closure

(i) Let y_1 and y_2 be real numbers.

$\begin{bmatrix} 1 & y_1 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 1 & y_2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & y_1 + y_2 \\ 0 & 2 \end{bmatrix} \notin$ H since 2 is a new entry.

Hence H is not closed under matrix addition.

Thus H does not form a group under matrix addition.

(ii) **Closure**

Let y_1 and y_2 be real numbers.

$\begin{bmatrix} 1 & y_1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & y_2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & y_1 + y_2 \\ 0 & 1 \end{bmatrix} \in$ H, $y_1 + y_2 \in \mathbb{R}$

Hence H is closed under matrix multiplication.

Assuming associativity.

Identity

The identity element is $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ since

$\begin{bmatrix} 1 & y_1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & y_1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & y_1 \\ 0 & 1 \end{bmatrix} \in$ H, where $y_1 \in \mathbb{R}$

Inverse

The inverse element is $\begin{bmatrix}1 & -y_1\\ 0 & 1\end{bmatrix}$ since

$$\begin{bmatrix}1 & y_1\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & -y_1\\ 0 & 1\end{bmatrix} = \begin{bmatrix}1 & -y_1\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & y_1\\ 0 & 1\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$$

Commutativity

For commutativity, we want to show that $a * b = b * a$

Let $y_1, y_2 \in \mathbb{R}$

LHS: $a * b = \begin{bmatrix}1 & y_1\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & y_2\\ 0 & 1\end{bmatrix} = \begin{bmatrix}1 & y_2 + y_1\\ 0 & 1\end{bmatrix} = \begin{bmatrix}1 & y_1 + y_2\\ 0 & 1\end{bmatrix}$

RHS: $b * a = \begin{bmatrix}1 & y_2\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & y_1\\ 0 & 1\end{bmatrix} = \begin{bmatrix}1 & y_1 + y_2\\ 0 & 1\end{bmatrix}$

LHS=RHS
Commutativity is satisfied hence H forms an Abelian group under matrix multiplication.

Example

To prove that the set S of all 2x2 invertible matrices with real entries forms a group under matrix multiplication.

Solution

Closure

Let $a,b,c,d,e,f,g,h \in \mathbb{R}$

$\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}e & f\\ g & h\end{pmatrix} = \begin{pmatrix}ae+bg & af+bh\\ ce+dg & cf+dh\end{pmatrix} \in S$ Hence S is closed under matrix multiplication

Associativity

For any three invertible 2x2 matrices A, B and C, it is known that A(BC) = (AB)C, thus the set S is associative with respect to multiplication.

"There are 10 kinds of people in the world, those that understand binary and the other 9" Jonathan Kariv

Identity

The identity element when multiplying 2x2 matrices is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \forall a, b, c, d \in \mathbb{R}$$

Inverse

Every element $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ of S has inverse $\frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

$$= \begin{pmatrix} \frac{d}{ad-bc} & \frac{b}{bc-ad} \\ \frac{c}{bc-ad} & \frac{a}{ad-bc} \end{pmatrix} \in S$$

Since the set S satisfies all the four group properties, it forms a group under matrix multiplication.

Commutativity

Let $a, b, c, d, e, f, g, h \in \mathbb{R}$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} e & f \\ g & h \end{pmatrix} \neq \begin{pmatrix} e & f \\ g & h \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ Hence the group is not commutative.

Exercise 1.2.2

1 A binary operation $\oplus$ is defined on the set $\mathbb{R}$ of real numbers by $x \oplus y = x - 5xy + y$. Determine if $\mathbb{R}$ forms a group under $\oplus$.

2 A set $G = \{i, -i, 1, -1\}$ is for complex numbers of unity moduli

(i) Construct a multiplication table for the elements.

(ii) Show that the set G forms a group under multiplication.

(iii) Explain briefly how the table shows that G is an Abelian group under multiplication

3 The set M consists of matrices of the form $\begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}$ where $n \in \mathbb{R}$. Determine whether $(M, *)$ forms a commutative group under matrix multiplication.

4 The elements of a group G are complex numbers $a + bi$ where $a, b \in \{0,1,2,3,4\}$. These elements are combined under the operation of addition modulo 5.

(a) State the identity element of G.

(b) Write down the inverse of $2 + 4i$.

5 The function f is defined by $f: x \mapsto \frac{1}{2-2x}$ for $x \in \mathbb{R}, x \neq 0, x \neq \frac{1}{2}, x \neq 1$. The function g is defined by $g(x) = ff(x)$.

(a) Show that $g(x) = \frac{1-x}{1-2x}$ and that $gg(x) = x$.

It is given that f and g are elements of a group K under the operation of composition of functions.

The element e is the identity, where $e: x \mapsto x$ for $x \in \mathbb{R}, x \neq 0, x \neq \frac{1}{2}, x \neq 1$.

(b) The inverse of the element f is denoted by h. Find $h(x)$.

(c) Construct the operation table for the elements e, f, g and h of the group K.

Miscellaneous Exercise 1.2

1 A binary operation $*$ is defined on the set $Q = \{a, b, c\}$ by the table below

$*$	$\boldsymbol{a}$	$\boldsymbol{b}$	$\boldsymbol{c}$
$\boldsymbol{a}$	b	a	c
$\boldsymbol{b}$	a	b	c
$\boldsymbol{c}$	c	c	b

Determine (a) whether or not Q is closed with respect to $*$.

(b) whether the operation is commutative,

(c) the identity element e, under the operation $*$,

(d) the inverse of each element.

2 Determine whether the given set S is, or is not a group under the given law of binary operation.

(a) Natural numbers: Multiplication

(b) Integers: addition

(c) Non-singular 2 x 2 matrices, Multiplication.

3 The elements of the set $P = \{1, 3, 9, 11\}$ are combined under the binary operation, $*$, defined as multiplication modulo 16.

(a) Demonstrate associativity for the elements $3, 9, 11$ in that order.

Assuming associativity holds in general, show that P forms a group under the binary operation $*$.

"There are 10 kinds of people in the world, those that understand binary and the other 9" Jonathan Kariv

(b) Write down all subgroups of P.

4 Define Q^+as the set of positive rational numbers. Prove that Q^+ forms an abelian group under the composition $*$ given as $a * b = \frac{a}{10}$, where $a, b \in Q^+$.

5 The binary operation $*$ is defined on the set $\mathbb{R}$ by $a * b = a + b + 4a^2b^2 \ \forall a, b \in \mathbb{R}$

Determine whether $*$ is (i) commutative, associative,

(ii) distributive over ordinary addition "+" of real numbers.

6 Consider the four matrices $\mathbf{E}, \mathbf{F}, \mathbf{G}$ and $\mathbf{H}$ where

$$\mathbf{E} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \mathbf{F} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \mathbf{G} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \mathbf{H} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$

Show that the set $\{\mathbf{E}, \mathbf{F}, \mathbf{G}, \mathbf{H}\}$ forms a group under the binary operation matrix multiplication.

State with a reason whether the set $\{\mathbf{E}, \mathbf{F}, \mathbf{G}, \mathbf{H}\}$ is an Albelian group.

7 A binary operation $*$ is defined on the set T= {0,1,2,3,4,5}

by $a * b = a + b - ab$, for all $a, b \in$ T on the table.
If $*$ denotes addition modulo 6,

$*$	**0**	**1**	**2**	**3**	**4**	**5**
0						
1						
2						
3						
4						
5						

gmanuwere@gmail.com /+263773975592/+263737967477

(i) copy and complete the table above.

(ii) Is the operation $*$ closed on T?

(iii) Find the identity element e under $*$.

Find the inverse of the element 2

8 A binary operation $\diamond$ is defined on a set M= $\{(p,q)$ such that $p,q \in \mathbb{R}\}$ by

$(p,q) \diamond (m,n) = (pm + 2qn, 2pq - q)$, for $m,n \in \mathbb{R}$.

(a) Find (i) $(2,3) \diamond (-4,1)$ (ii) $(-4,1) \diamond (2,3)$

What conclusion can you draw from the result of (i) and (ii).

(b) Find the values of x and y if $(x,1) \diamond (2,y) = (1,1) \diamond (2,1)$.

9 M is the set os all 2x2 matrices of the form $\begin{pmatrix} a & b \\ 0 & \frac{1}{a} \end{pmatrix}$, $a \neq 0$, where a and b are rational numbers.

(a) Show that under matrix multiplication M is a group. You may assume associativity of matrix multiplication.

(b) Determine whether the group is commutative.

10 The binary operations $*$ and $\otimes$ are defined on the set $\mathbb{R}$ of real numbers by

$a * b = a + 2b + 4, \forall a, b \in \mathbb{R}$ and $a \otimes b = a + 3b - ab, \forall a, b \in \mathbb{R}$

Find the value of

(a) $2 * (3 \otimes 5)$ (b) $(2 * 3) \otimes (2 * 5)$

(c) What conclusion can you draw from the result of (a) and (b).

11 Show that the set $G = \{1, 5, 7, 11\}$ under the binary operation of multiplication modulo 12, is a group. State whether or not the set is an Abelian group.

12 A binary operation $*$ is defined on the set $\mathbb{R}$, of real numbers by $p * q = pq - 3\sqrt{3}$, where $p, q \in \mathbb{R}$.

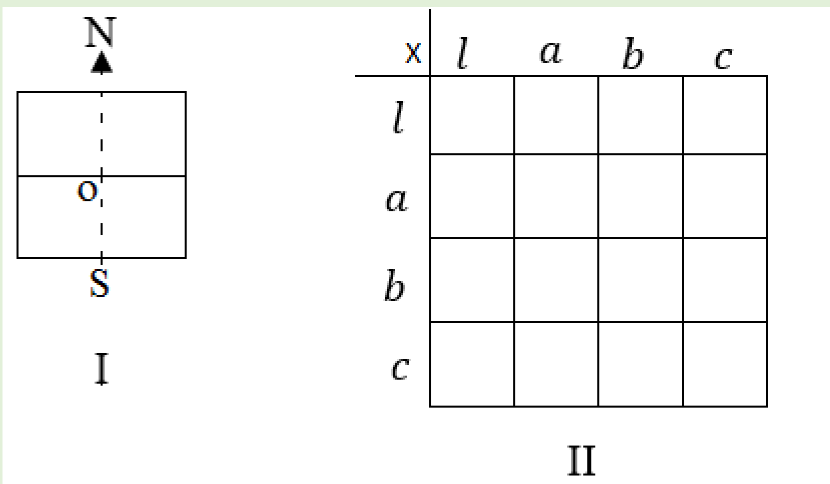
(a) Evaluate $(\sqrt{3}+1) * (\sqrt{3}-1)$

(b) Find (i) the identity element e of $\mathbb{R}$ under the operation $*$,

(ii) the inverse p^{-1} of p,

(iii) The inverse of $3\sqrt{3}$.

13



(a) The operations below are performed on the square above to produce elements of the set $= \{l, a, b, c\}$, where

$l =$ leave the square where it is,

$a =$ rotate it through 90° anticlockwise about O,

$b =$ rotate it through 180° anticlockwise about O,

$c =$ rotate it through 90° clockwise about O.

The x sign means "followed by" binary operation on the set S elements.

Make use of square I and the meanings of the elements, to complete table II. Copy and fill up the table above. State the inverse of a.

(b) The set G = {0, 1, 2, 3}. Show that the set G forms a group under the operation of addition modulo 4.

14 A binary operation $\odot$ defined on a set $Q = \{2,3,4,5\}$ has operation table shown.

$\odot$	**2**	**3**	**4**	**5**
2	2	3	4	5
3	3	4	5	2
4	4	5	1	3
5	5	1	3	4

(a) Determine whether or not

(i) Q is closed with respect to the binary operation $\odot$,

(ii) the operation $\odot$ is commutative.

(b) What is the identity element e, under the operation $\odot$.

15 Find the matrices for the clockwise rotations about the origin through the angles $0°, 90°, 180°, 270°$.

By constructing a table of compositions show that this set denoted by M forms a group under matrix multiplication.

16 The binary operation $*$ is defined on the set $\mathbb{R}$ of real numbers by $a * b = a + b + 3ab, \forall a, b \in \mathbb{R}$.

Find

(a) $3a * 5b$ (b) $(x^2 + x + 1) * x$ (c) $(a * b) * c$ (d) $a * (b * c)$

(e) what can you conclude about your answers for part (c) and (d)?

17 Show that the set $P = \{1, 3, 4, 5, 9\}$ under the binary operation of multiplication modulo 11, is a group.

18 A binary operation $*$ is defined on the set $\mathbb{R}$ of real numbers by $p * q = p + q - 3pq$ where $p, q \in \mathbb{R}$.

Find (a) the identity element e under the operation (b) the inverse of an element $x \in \mathbb{R}$

“There are 10 kinds of people in the world, those that understand binary and the other 9” Jonathan Kariv

19 A set G = {0,1,2,3,4}, where the elements are defined from the turning of a minute hand of a clock as follows:

0 = a turn through 0 minutes or multiples of 60 minutes

1 = turn through 12 minutes

2 = turn through 24 minutes

3 = turn through 36 minutes

4 = turn through 48 minutes

Defining $a * b$ as "a turn of the element a followed by a turn of the element b".

(i) Construct a multiplication table for all the elements of the set G.

(ii) Show that the set G is a group.

(iii) Establish whether the set G forms an Abelian group. Give a reason for your answer.

20 The binary operation $*$ is defined on the set $\mathbb{R}$ of real numbers by $a * b = a + ab^2 + 3, \forall a, b \in \mathbb{R}$.

Find (a) $(5 * 3) * 7$ (b) $5 * (3 * 7)$

(c) What conclusion can you draw from the results of (a) and (b).

21 Consider the set $H = \{1, 3, 5, 7\}$ under the binary operation of multiplication modulo 8.

(i) Construct the operation table and, assuming associativity, show that H forms a group.

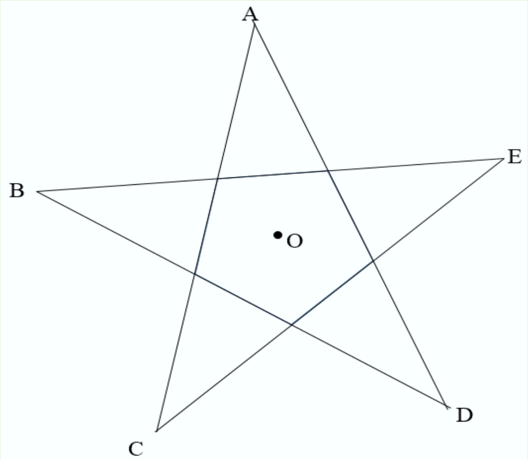
(ii) Find all the proper subgroups of G.

22 The binary operation $*$ is defined on the set $\mathbb{R}$ of real numbers by $a * b = \frac{a+b}{2ab}$. $\forall a, b \in \mathbb{R}$. Find

(a) $a * (b * c)$ (b) $(a * b) * c$ (c) $(2x + 1) * (3x + 2)$ (d) $\frac{3}{3a*5b}$

"There are 10 kinds of people in the world, those that understand binary and the other 9" Jonathan Kariv

23



The diagram shows a regular pentagon ABCDE with centre O. Five transforms of the figure are defined as follows:

e is the volentity transformation "do nothing".

r_1, r_2, r_3, r_4 are anticlockwise rotations about O through $\frac{2\pi}{5}, \frac{4\pi}{5}, \frac{6\pi}{5}, \frac{8\pi}{5}$, respectively.

Given that the five transformations form a group, construct the corresponding group table. State the inverse of each transformation.

gmanuwere@gmail.com /+263773975592/+263737967477