PARUL UNIVERSITY
FACULTY OF ENGINEERING & TECHNOLOGY
Department of Applied Sciences & Humanities
Third Semester B. Tech (CSE, IT)
Discrete Mathematics (303191202)
Unit 4 - Algebraic Structures & Morphisms
Academic Year: 2025-26

Introduction:

In mathematics and abstract algebra, group theory studies the algebraic structures known as groups. The concept of a group is central to abstract algebra: other well-known algebraic structures, such as rings, fields, and vector spaces, can all be seen as groups endowed with additional operations and axioms. Groups recur throughout mathematics, and the methods of group theory have influenced many parts of algebra. Linear algebraic groups and Lie groups are two branches of group theory that have experienced advances and have become subject areas in their own right.

Prerequisites:

- Basic familiarity with the concept of sets, functions
- Reasonable comfort with the use of symbols to denote sets, elements and operations.
- An ability to manipulate algebraic expressions based on fixed rules.
- An ability to carry out logical reasoning in the mind and on paper, and follow reasoning carried out by others.

Application:

Group theory, the ultimate theory for symmetry, is a powerful tool that has a direct impact on research in robotics, computer vision, computer graphics and medical image analysis.

In theoretical computer science:

- Minimizing space usage of algorithms
- Quantum algorithms
- Cryptography: Fully homomorphic encryption, obfuscation,…
- Mulmuley's approach to P vs.NP
- Babai's algorithm for Graph Isomorphism
- Derandomization

In puzzles and games:

- "15 Puzzle"
- Rubik's cube
- Tangles…

In Physics:

- Predicting the existence of elementary particles before they are discovered

In Chemistry

- The structure and behaviour of molecules and crystals depends on their different symmetries.

Overview:

- Semigroup; Monoid; Group
- Congruence relation
- Free & cyclic monoid & group
- Permutation groups
- Subgroups; Normal subgroup
- Rings; Integral domain & fields
- Boolean algebra and Boolean ring
- Identity of Boolean algebra
- Duality
- Representation of Boolean function
- Disjunctive and Conjunctive Normal form

Weightage: 40%

Teaching Hours: 18

GROUPS

Binary operation:
Let A be a set. A function $f: A \times A \longrightarrow A$ is called a binary operator on the set A.

Algebraic structure:
An algebraic structure is an ordered tuple: $(S, \circ_1, \circ_2, \ldots, \circ_n)$ where S is a set which has one or more binary operations $\circ_1, \circ_2, \ldots, \circ_n$ defined on all the elements of $S \times S$.
An algebraic structure with one (binary) operation is thus an ordered pair which can be denoted by $(S, \circ)$ or $(T, *)$, and so on.

Definitions:
Let G be a set and $*$ be an operation on G.
Consider the following properties on G with the operation $*$.

(i)	Closure property:	For any $a, b \in G$, $a * b \in G$. $[i.e.\ G$ is closed under the operation $*]$ $[i.e.*$ is a binary operation on $G.]$
(ii)	Associativity:	For any $a, b, c \in G$; $a * (b * c) = (a * b) * c$. $[i.e.*$ is associative on $G.]$
(iii)	Identity Element:	There exists an element e ***in*** G such that $a * e = e * a = a$ for every $a \in G$. e is called the identity element of G under the operation $*$
(iv)	Inverse element:	Let e be the identity element of G under the operation $*$ For any $a \in G$, there exists an element b ***in*** G such that $a * b = b * a = e$. b is called the inverse element of a under the operation $*$. It is denoted by a^{-1}.
(v)	Commutative property:	For any $a, b \in G$, $a * b = b * a$.

$(G, *)$ is said to be a ***Semigroup*** if it satisfies the properties $(i), (ii)$.
$(G, *)$ is said to be a ***Monoid*** if it satisfies the properties $(i), (ii), (iii)$.
$(G, *)$ is said to be a ***Group*** if it satisfies the properties $(i), (ii), (iii), (iv)$.
$(G, *)$ is said to be an ***Abelian group*** if it satisfies the properties $(i), (ii), (iii), (iv), (v)$.

A group is said to be a **finite group** if it has finite number of elements. The cardinality of the set is known as the order of that group.
If a group is not finite, it is said to be an **infinite group**.

Problem.1. Prove that $\mathbb{Z}$, the set of integers is an abelian group under the operation of the usual addition of integers. **[Summer_2023-24]**

Solution:

(i)	Closure property:	Clearly, addition of two integers is an integer. $i.e.$ For any $a, b \in \mathbb{Z}$, $a + b \in \mathbb{Z}$. Hence, $\mathbb{Z}$ is closed under the operation $+$
(ii)	Associativity:	For any $a, b, c \in \mathbb{Z}$; $a + (b + c) = (a + b) + c$. Hence, $+$ is associative on $\mathbb{Z}$
(iii)	Identity Element:	We know that $0 \in \mathbb{Z}$ such that $a + 0 = 0 + a = a$ for every $a \in \mathbb{Z}$. Hence, 0 is called the identity element of $\mathbb{Z}$ under the operation $+$
(iv)	Inverse element:	For any $a \in \mathbb{Z}$, there exists an element $-a$ ***in*** $\mathbb{Z}$ such that $a + (-a) = (-a) + a = 0$. Therefore, **every** element a in $\mathbb{Z}$ has an inverse element $-a$ **in** $\mathbb{Z}$.
(v)	Commutative property:	For any integers $a, b \in \mathbb{Z}$, $a + b = b + a$.

Since, all the five properties are satisfied, $\mathbb{Z}$ is an abelian group under $+$.

Problem.2.

Check if the set of all real $m \times n$ matrices is an abelian group under the usual addition of matrices.

Solution:

Let $M_{m\times n}$ be the set of all real $m \times n$ matrices and let $+$ denote the usual addition of matrices.

(i)	Closure property:	Clearly, addition of $m \times n$ matrices is an $m \times n$ matrix. $i.e.$ For any $A, B \in M_{m\times n}$, $A + B \in M_{m\times n}$. Hence, $M_{m\times n}$ is closed under the operation $+$
(ii)	Associativity:	For any $m \times n$ matrix $A = [a_{ij}], B = [b_{ij}], C = [c_{ij}]$ in $M_{m\times n}$ $A + (B + C) = [\mathrm{a_{ij}} + (\mathrm{b_{ij}} + \mathrm{c_{ij}})]$ $= [(\mathrm{a_{ij}} + \mathrm{b_{ij}}) + \mathrm{c_{ij}}] \quad [\because a_{ij}, b_{ij}, c_{ij} \in \mathbb{R}]$ $= (A + B) + C$ Hence, $+$ is associative on $M_{m\times n}$.
(iii)	Identity Element:	Let $0_{m\times n} \in M_{m\times n}$ be an $m \times n$ matrix with all entries to be 0. Then for any $A = [a_{ij}]$ in $M_{m\times n}$, $A + 0_{m\times n} = [a_{ij}] + [0] = [a_{ij} + 0] = [a_{ij}] = A$ $0_{m\times n} + A = [0] + [a_{ij}] = [0 + a_{ij}] = [a_{ij}] = A$ Hence, $0_{m\times n}$ is the identity element of $M_{m\times n}$under the operation $+$
(iv)	Inverse element:	For any $A = [a_{ij}] \in M_{m\times n}$, consider the $m \times n$ matrix $-A = [-a_{ij}]$ Then $A + (-A) = [a_j + (-a_{ij})] = [0] = 0_{m\times n}$ and $(-A) + A = 0_{m\times n}$ Therefore, **every** element $A = [a_{ij}]$ in $M_{m\times n}$ has an inverse element $-A = [-a_{ij}]$ **in** $M_{m\times n}$.
(v)	Commutative property:	For any $m \times n$ matrices $A = [a_{ij}], B = [b_{ij}] \in M_{m\times n}$, $A + B = [\mathrm{a_{ij}} + \mathrm{b_{ij}}]$ $= [\mathrm{b_{ij}} + \mathrm{a_{ij}}] \quad [\because a_{ij}, b_{ij}, c_{ij} \in \mathbb{R}]$ $= B + A$

Hence, $M_{m\times n}$ is an abelian group under the operation of matrix addition.

Problem.3.
Check if the set of all non-negative integers is an abelian group under usual addition of integers.

Solution:
Consider the set $\mathbb{N} \cup \{0\}$ of all non-negative integers.

(i)	Closure property:	Clearly, addition of two non-negative integers is a non-negative integer. $i.e.$ For any $a, b \in \mathbb{N} \cup \{0\}$, $a + b \in \mathbb{N} \cup \{0\}$. Hence, $\mathbb{N} \cup \{0\}$ is closed under the operation $+$
(ii)	Associativity:	For any $a, b, c \in \mathbb{N} \cup \{0\}$; $a + (b + c) = (a + b) + c$. Hence, $+$ is associative on $\mathbb{N} \cup \{0\}$
(iii)	Identity Element:	We know that $a + 0 = 0 + a = a$ for every $a \in \mathbb{N} \cup \{0\}$. Hence, 0 is called the identity element of $\mathbb{N} \cup \{0\}$ under the operation $+$
(iv)	Inverse element:	For $1 \in \mathbb{N} \cup \{0\}$, -1 is the only integer that gives $1 + (-1) = (-1) + 1 = 0$ But $-1 \notin \mathbb{N} \cup \{0\}$. Thus, there is an element in $\mathbb{N} \cup \{0\}$ which does not have an inverse element in $\mathbb{N} \cup \{0\}$ under $+$. Hence, this property is not satisfied.
(v)	Commutative property:	For any non-negative integers $a, b \in \mathbb{N} \cup \{0\}$, $a + b = b + a$.

Since, all the five properties are not satisfied, $\mathbb{N} \cup \{0\}$ **is not an abelian group** under $+$.
But, since properties $(i), (ii), (iii)$ and (v) are satisfied it **is an abelian monoid**.

Problem.4.
Check if the set of all natural numbers is an abelian group under usual addition of integers.
Solution:
Consider the set $\mathbb{N}$ of all natural numbers.

(i)	Closure property:	Clearly, addition of two natural numbers is a natural number. $i.e.$ For any $a, b \in \mathbb{N}$, $a + b \in \mathbb{N}$. Hence, $\mathbb{N}$ is closed under the operation $+$
(ii)	Associativity:	For any $a, b, c \in \mathbb{N}$; $a + (b + c) = (a + b) + c$. Hence, $+$ is associative on $\mathbb{N}$
(iii)	Identity Element:	0 is the only integer such that $a + 0 = 0 + a = a$ for every $a \in \mathbb{N}$. But $0 \notin \mathbb{N}$. Hence, $\mathbb{N}$ has no identity element under the operation $+$
(iv)	Inverse element:	For $1 \in \mathbb{N}$, -1 is the only integer that gives $1 + (-1) = (-1) + 1 = 0$ But $-1 \notin \mathbb{N}$. Thus, there is an element in $\mathbb{N}$ which does not have an inverse element in $\mathbb{N}$ under $+$. Hence, this property is not satisfied.
(v)	Commutative property:	For any $a, b \in \mathbb{N}$, $a + b = b + a$.

Since, properties (iii) &(iv) are not satisfied, $\mathbb{N}$ **is not an abelian group** under $+$.
But, since properties $(i), (ii)$ and (v) are satisfied it **is an abelian semigroup**.
Note that it is neither a monoid nor a group.

Problem.5.

Check if the set of integers $\mathbb{Z}$ is an abelian **semigroup** under the operation of the usual subtraction of integers. Also check for the identity element and the commutative property.

Solution:

(i)	Closure property:	Clearly, subtraction of two integers is an integer. $i.e.$ For any $a, b \in \mathbb{Z}$, $a - b \in \mathbb{Z}$. Hence, $\mathbb{Z}$ is closed under the subtraction $\cdot$
(ii)	Associativity:	For $1,2,3 \in \mathbb{Z}$, $1 - (2 - 3) = 1 - (-1) = 2$ and $(1 - 2) - 3 = (-1) - 3 = -4$ $i.e.$ for some $a, b, c \in \mathbb{Z}$, $a - (b - c) \neq (a - b) - c$. Hence, this property is not satisfied.

Since, property (ii) is not satisfied, $\mathbb{Z}$ is not a semigroup.

Identity Element:	We know that for any $e \in \mathbb{Z}$, $a - e \neq e - a = a$ for every non-zero $a \in \mathbb{Z}$. $i.e.$ there exists no $e \in \mathbb{Z}$ such that $a - e = e - a = a$, for all $a \in \mathbb{Z}$ Hence, $\mathbb{Z}$ has no identity element of under the operation subtraction.
Commutative property:	For any non-zero integers $a, b \in \mathbb{Z}$, $a - b \neq b - a$. Hence, this property is not satisfied.

Problem.6.

Check if the set of integers $\mathbb{Z}$ is an abelian group under the operation of the usual multiplication

Solution:

(i)	Closure property:	Clearly, multiplication of two integers is an integer. $i.e.$ For any $a, b \in \mathbb{Z}$, $a \cdot b \in \mathbb{Z}$. Hence, $\mathbb{Z}$ is closed under the operation $\cdot$
(ii)	Associativity:	For any $a, b, c \in \mathbb{Z}$; $a \cdot (b \cdot c) = (a \cdot b) \cdot c$. Hence, $\cdot$ is associative on $\mathbb{Z}$.
(iii)	Identity Element:	We know that $1 \in \mathbb{Z}$ such that $a \cdot 1 = 1 \cdot a = a$ for every $a \in \mathbb{Z}$. Hence, 1 is called the identity element of $\mathbb{Z}$ under the operation $\cdot$
(iv)	Inverse element:	For $0 \in \mathbb{Z}$, there exists no integer b $\boldsymbol{in}$ $\mathbb{Z}$ such that $0 \cdot b = b \cdot 0 = 1$. Therefore, $0 \in \mathbb{Z}$ does not have an inverse element in $\mathbb{Z}$. Thus, there is an element in $\mathbb{Z}$ which does not have an inverse element under $\cdot$ Hence, this property is not satisfied.
(v)	Commutative property:	For any integers $a, b \in \mathbb{Z}$, $a \cdot b = b \cdot a$.

Since, property (iv) is not satisfied, $\mathbb{Z}$ is not an abelian group under multiplication.
But, it is an abelian monoid under multiplication.

Exercise

1. Check if the set of all real numbers is commutative group under usual addition.
2. Check if the set of all real numbers is commutative group under usual multiplication.
3. Check if the set of all non-zero real numbers is commutative group under usual addition.
4. Check if the set of all real numbers is commutative group under usual subtraction.
5. Check if division is a binary operation on the set of all real numbers.
6. Prove that the set of all non-zero real numbers is not a semigroup under usual division. Do the other properties hold to make it an abelian group?
7. If * is defined on $\mathbb{Z}$ such that a*b = a+b+2 ,Prove that ($\mathbb{Z}$, *) is an abelian Group. [Summer_2018-19]

Definition:
If for an element a in an algebraic structure$(G,*)$, $a^2 = a * a = a$ then a is said to be the idempotent element in $(G,*)$.

For example:
Show that the following are idempotent elements under the given operations.
(i) $\emptyset$ for union and intersection of two sets
(ii) 0 for + on $\mathbb{Z}$
(iii) 1 for multiplication on $\mathbb{R}$

Solution:
(i) Since $\emptyset \cup \emptyset = \emptyset$, $\emptyset$ is idempotent under union.
Since $\emptyset \cap \emptyset = \emptyset$, $\emptyset$ is idempotent under intersection.
(ii) Since $0 + 0 =$, 0 is idempotent under + on $\mathbb{Z}$.
(iii) Since $1 \cdot 1 = 1$, 1 is idempotent under multiplication on $\mathbb{R}$.

Problem.1.

In each of the following cases, prove that $\mathbb{Z}$ under the operation $*$ is not an abelian group.
[Winter_2022-23, Winter_2019-20]
(a) $a * b = \frac{a}{b}$ (b) $a * b = 20$ (c) $a * b = 2a - b$ (d) $a * b = |a + b|$

Solution:
(a) $a * b = \frac{a}{b}$ over $\mathbb{Z}$
For $a = 1, b = 2$, $a * b = \frac{a}{b} = \frac{1}{2} \notin \mathbb{Z}$.
Hence, closure property is not satisfied.
It does not form a group.

(b) $a * b = 20$ over $\mathbb{Z}$
For any $a \in \mathbb{Z}$ there is no element e in $\mathbb{Z}$ such that $a * e = e * a = a$
Hence, identity element does not exist.
It does not form a group.

(c) $a * b = 2a - b$ over $\mathbb{Z}$
For $a = 1, b = 2, c = 3$,
$$a * (b * c) = 1 * (2 * 3) = 1 * (2(2) - 3) = 1 * 1 = 2(1) - 1 = 1$$
$$(a * b) * c = (1 * 2) * 3 = (2(1) - 2) * 3 = 0 * 3 = 2(0) - 3 = -3$$
Thus, $a * (b * c) \neq (a * b) * c$
Hence, associative property is not satisfied.
It does not form a group

(d) $a * b = |a + b|$ over $\mathbb{Z}$
For $a = -1, b = -2, c = -3$
$$a * (b * c) = (-1) * (-2 * -3) = (-1) * (|-2 - 3|) = (-1) * 5 = |-1 + 5| = 4$$
$$(a * b) * c = (-1 * -2) * (-3) = (|-1 - 2|) * (-3) = 3 * (-3) = |3 + (-3)| = 0$$
Thus, $a * (b * c) \neq (a * b) * c$
Hence, associative property is not satisfied.
It does not form a group

Problem.2.
Identify the identity element in $\mathbb{Z}$ under the operation $*$ given as $a * b = a + b - 2$, for any $a, b \in \mathbb{Z}$. Also identify the inverse element of any member $a \in \mathbb{Z}$ **[Winter_2022-23]**
Solution:
$a * b = a + b - 2 = b + a - 2 = b * a$, for any $a, b \in \mathbb{Z}$.
Identity Element:
Let e be such that $a * e = a = e * a$
Now, $a * e = a \Longrightarrow a + e - 2 = a \Longrightarrow e = 2$ which belongs to $\mathbb{Z}$.
Hence, $e = 2$ is the identity element in $\mathbb{Z}$ under the given operation.
Inverse element:
Let $a \in \mathbb{Z}$.and b be such that $a * b = e = b * a$.
$a * b = e \Longrightarrow a + b - 2 = 2 \Longrightarrow b = 4 - a$ which belongs to $\mathbb{Z}$
Hence, $4 - a$ is the inverse of any element a in $\mathbb{Z}$ under the given operation.

Problem.3
If f: $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ where $\mathbb{Z}$ is the set of integers and $f(x, y) = x * y = x + y - xy$,
Show that the binary operation $*$ is commutative and associative.
Find the identity element and inverse of each element. **[Summer_2023-24]**
Solution.

- **Commutative property :**
  Let $x, y \in \mathbb{Z}$
  $$x * y = x + y - xy = y + x - yx = y * x$$
- **Associative property:**
  Let $x, y, z \in \mathbb{Z}$
  $$\begin{aligned}(x * y) * z &= (x * y) + z - (x * y)z \\ &= (x + y - xy) + z - (x + y - xy)z \\ &= x + y - xy + z - xz - yz + xyz \\ &= x + y + z - yz - xy - xz + xyz \\ &= x + (y + z - yz) - x(y + z - yz) \\ &= x + (y * z) - x(y * z) \\ &= x * (y * z)\end{aligned}$$
- **Identity element**:
  Suppose $e \in \mathbb{Z}$ is an identity element, then by definition
  $a * e = a \Longrightarrow a + e - ae = a \Longrightarrow (1 - a) = 0$
  Either $e = 0$ or $1 - a = 0$
  But $1 - a \neq 0$ because a is arbitrary element
  Therefore $e = 0$ is the identity element.

- **Inverse element:**
  Let $a \in \mathbb{Z}$ be any arbitrary element, and let $b \in \mathbb{Z}$ be the inverse of a.
  Then by definition, $a * b = b * a = e$
  $$\begin{aligned}a * b = e &\Longrightarrow a + b - ab = 0 \\ &\Longrightarrow a + b(1 - a) = 0 \\ &\Longrightarrow b(1 - a) = -a \\ &\Longrightarrow b = \frac{-a}{1 - a}, a \neq 1 \\ &\Longrightarrow b = \frac{a}{a - 1}, a \neq 1\end{aligned}$$
  But $\frac{a}{a-1} \in \mathbb{Z}$, $for\ a = 0,2$
  But, for $a \neq 0,2, a^{-1}$ does not exist under $*$

Problem.4

If $*$ is a binary operation on $\mathbb{Z}^+$ of positive integers, defined by $a * b = lcm(a, b)$

1. Show that $*$ is commutative and associative
2. Which element of $\mathbb{Z}^+$ are idempotent
3. Find the identity element of $\mathbb{Z}^+$ $w.r.t$ $*$
4. Which elements of $\mathbb{Z}^+$ have inverse?

Solution

1. **Commutative property :**
   $a * b = lcm(a, b) = lcm(b, a) = b * a$
   i.e $*$ is commutative.
   Associative property:
   $$\begin{aligned} a * (b * c) &= a * lcm(b, c) \\ &= lcm\big(a, lcm(b, c)\big) \\ &= lcm(a, b, c) \\ &= lcm(lcm(a, b), c) \\ &= lcm(a, b) * c \\ &= (a * b) * c \end{aligned}$$
   Hence, $*$ is associative.
2. **For any element $a \in \mathbb{Z}+$**, $a * a = (a, a) = a$. Hence, every element is idempotent.
3. **For any element $a \in \mathbb{Z}+$**, $a * 1 = (a, 1) = a$ Hence, 1 is the identity element.
4. If b is inverse of an element a, then $a * b = 1$. i.e. $(a, b) = 1$
   But $lcm(a, b) = 1$ if and only if $a = b = 1$
   Hence, only $1 \in \mathbb{Z}^+$ has an inverse.
   No other element has an inverse in $\mathbb{Z}^+$ under the given operation.

Problem.5

Show that the binary operation on the set of natural numbers given by $a * b = a$ is not commutative but is associative.

Solution

For commutative property:

Consider two natural numbers $1 and\ 2$.
Then $1 * 2 = 1$ and $2 * 1 = 2$
Thus, $1 * 2 \neq 2 * 1$.
Hence, $*$ is not commutative.

For associative property:

Let a, b, c be any natural numbers. Then
$a * (b * c) = a * b = a$ and $(a * b) * c = a * c = a$
Hence, $a * (b * c) = (a * b) * c$
Therefore, $*$ is associative.

Problem.6.

The identity element in $\mathbb{Z}$ under the operation $*$ given as $a * b = a + b - 4$, for any $a, b \in \mathbb{Z}$. is ___
[Summer_2023-24]

Problem.7.

Which of the flowing set is not an abelian semi-group under given operations? **[Summer_2023-24]**
(a) $(Q - \{0\}, \times)$ (b) $(Z, +)$ (c) $(Z, -)$ (d) $(R, +)$

1.R is not a Group under usual multiplication × because **[Winter_2022-23]**
(a) × is not associative on R
(b)Identity element does not exists in R with respect to ×
(c) Inversion property is not satisfied
(d) R is not closed under ×.

2. If a group satisfies the Closure , Associative and identity property then it is known as **[Winter_2022-23]**
(a) Abelian Group
(b) Symmetric group
(c) Semigroup
(d) Monoid

Exercise:

1) Verify whether the usual multiplication on the set $S = \{-1, 1\}$ is a binary operation.
2) Determine whether the operation $*$ on the set of natural numbers given $a * b = \frac{a+b}{ab}$ is a binary operation. **[Winter_20121-22]**
3) Show that the binary operation $*$ defined on $\mathbb{R}$ by $a * b = max(a, b)$ is associative
4) Show that the binary operation $*$ defined on the set of rational numbers Q defined as $a * b = \frac{ab}{2}$ is both commutative and associative.
5) Examine whether matrix multiplication on the set $M = \left\{\begin{bmatrix} 0 & a \\ b & 0 \end{bmatrix} : a, b \in \mathbb{R}\right\}$ of matrices is a binary operation.

Theorem: Uniqueness of identity element in an algebraic structure $(G,*)$.

Statement: If an algebraic structure $(G,*)$ has an identity element then it is unique.
Proof: Let e_1 and e_2 be two identity elements of $(G,*)$.
e_1 is an identity element, therefore for every $a \in G$, $a * e_1 = a = e_1 * a$ ----------(i)
Since $e_2 \in G$, using (i), $e_2 * e_1 = e_2 = e_1 * e_2$. ----------$(ii)$
e_2 is an identity element, therefore for every $a \in G$, $a * e_2 = a = e_2 * a$ ----------(iii)
Since $e_1 \in G$, using (iii), $e_1 * e_2 = e_1 = e_2 * e_1$ ----------(iv)
From (ii) and (iv), $e_2 = e_1 * e_2 = e_1$
Hence, proved.

Theorem: Uniqueness of inverse element in a group $(G,*)$.
Statement: If $(G,*)$ is a group then every $a \in G$ has a unique inverse.
Proof:
Let $(G,*)$ be a group with identity element e.
Let $a \in G$ be any element of G.
Let $b, c \in G$ be inverse elements of a.
Then by definition,
$a * b = b * a = e$ and $a * c = c * a = e$.

$$
\begin{aligned}
\text{Now, } b &= b * e && [\because e \text{ is identity element}] \\
&= b * (a * c) && [\because c \text{ is inverse of } a] \\
&= (b * a) * c && [\because \text{associative property holds}] \\
&= e * c && [\because c \text{ is inverse of } a] \\
&= c && [\because e \text{ is identity element}]
\end{aligned}
$$

Hence, proved.

Theorem: Left cancellation law for Groups.
Statement : Let $(G,*)$ be a group and a, b, c be elements of G. If $ab = ac$ then $b = c$.
Proof : Since $(G,*)$ is a group a^{-1} exists in G. Let e be the identity element of G.

$$\begin{aligned} ab = ac &\Rightarrow a^{-1}(ab) = a^{-1}(ac) && [Multiplying\ both\ sides\ by\ a^{-1}] \\ &\Rightarrow (a^{-1}a)b = (a^{-1}a)c && [Associative\ property] \\ &\Rightarrow eb = ec && [definition\ of\ inverse\ element] \\ &\Rightarrow b = c && [definition\ of\ identity\ element] \end{aligned}$$

Hence, proved.

Theorem: Right cancellation law for Groups.
Statement : Let $(G,*)$ be a group and a, b, c be elements of G. If $ba = ca$ then $b = c$.
Proof : Since $(G,*)$ is a group a^{-1} exists in G. Let e be the identity element of G.

$$\begin{aligned} ba = ca &\Rightarrow (ba)a^{-1} = (ca)a^{-1} && [Multiplying\ both\ sides\ by\ a^{-1}] \\ &\Rightarrow b(aa^{-1}) = c(aa^{-1}) && [Associative\ property] \\ &\Rightarrow be = ce && [definition\ of\ inverse\ element] \\ &\Rightarrow b = c && [definition\ of\ identity\ element] \end{aligned}$$

Theorem: If G is a group, $a \in G$ and $b \in G$ then $(i)(a^{-1})^{-1} = a$ and $(ii)(ab)^{-1} = b^{-1}a^{-1}$.

Proof:
(i) Clearly, for any $\in G$, by definition $aa^{-1} = a^{-1}a = e$. Hence, $(a^{-1})^{-1} = a$
(ii) $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a(e)a^{-1} = aa^{-1} = e$
Similarly, $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}(e)b = b^{-1}b = e$.
Hence, $(ab)^{-1} = b^{-1}a^{-1}$.

Congruence Relation

When an integer A is divided by an integer B, it gives an equation that looks like

$$\boldsymbol{A = Q \,.\, B + R}$$

A is the dividend
B is the divisor
Q is the quotient
R is the remainder
Focusing on the remainder only, and using the modulo operator (abbreviated as mod), it can be written as $A \equiv R \ (mod\ B)$.

Definition:
Let a, b, m be integers.
If $a - b$ is divisible by m then a and b are said to be $congruent\ modulo\ m$".
It is written as $a \equiv b(mod\ m)$.
For example,
$16 - 4 = 12$ is divisible by 3 therefore we write $16 \equiv 4(mod\ 3)$.
$227 - 2$ is divisible by 3 therefore we write $227 \equiv 2(mod\ 3)$.
$227 - 2$ is not divisible by 4 therefore we write $227 \not\equiv 2(mod\ 4)$
Note:

$$\begin{aligned} a \equiv b(mod\ m) &\Leftrightarrow a - b\ is\ divisible\ by\ m \\ &\Leftrightarrow m\ divides\ (a - b) \\ &\Leftrightarrow a - b = km, for\ some\ integer\ k \\ &\Leftrightarrow \frac{a - b}{m}\ is\ an\ integer \end{aligned}$$

Problem.1. Prove that the relation "$congruence\ modulo\ m$" is an equivalence relation.
Solution.
We say that aRb if $a \equiv b(mod\ m)$ for some fixed integer m.

(i)	**Reflexive**	$a - a = 0$ is divisible by m, because $0 = 0 \cdot m$. Hence, $a \equiv a\ (mod\ m)$, $i.e.\ aRa$. So $congruence\ modulo\ m$ is reflexive
(ii)	**Transitive**	For any integers a, b, c, let aRb, bRc $\therefore a \equiv b(mod\ m)$ and $b \equiv c(mod\ m)$ $\therefore m$ divides $a - b$ and m divides $b - c$. $i.e.\ a - b = km$ and $b - c = lm$, for some integers k, l. Now, $a - c = (a - b) + (b - c) = km + lm = (k + l)m$. $\therefore m$ divides $a - c$. Hence, $a \equiv c(mod\ m)$ Thus, $aRb, bRc \Longrightarrow aRc$. Hence, $congruence\ modulo\ m$ is transitive.
(iii)	**Symmetric**	For any integers a, b, $a \equiv b(mod\ m) \Longrightarrow m$ divides $(a - b)$ $\Longrightarrow a - b = km$, for some integer k $\Longrightarrow b - a = (-k)m$, for some integer $-k$ $\Longrightarrow m$ divides $(b - a)$ $\Longrightarrow b \equiv a(mod\ m)$ Hence, $congruence\ modulo\ m$ is symmetric.

Hence, proved.

Properties of the relation "$congruence\ modulo\ m$" :

- If $a \equiv b(mod\ m)$and $c \equiv d(mod\ m)$ then the following are true for any integers l, k and n.
  (i) $a \pm c \equiv (b \pm d)(mod\ m)$
  (ii) $ac \equiv (bd)(mod\ m)$
  (iii) $ka \equiv kb(mod\ m)$

QUOTIENT STRUCTURE

Consider an algebraic structure $(G,*)$ with an equivalence relation say R.
Two elements a, b are said to be equivalent to each other if $(a, b) \in R$.
A collection of all equivalent elements is called Equivalence class. Thus, elements a and b belong to the same **equivalence class** if and only if a and b are equivalent.
Thus, the equivalence class of an element a in G is the set $\{x \in G\ |xRa\}$
Every element of G will be a member of some unique equivalence class.
Thus, the set of all equivalence classes gives a partition of G.
This partition is known as quotient structure of G. It is denoted by G/R.

Definition:
Let $(G,*)$ be an algebraic structure and R be an equivalence relation on it. The set of all equivalence classes of G given by R is known as the quotient structure of G.

For example, consider the group of integers $(\mathbb{Z}, +)$ with the relation "$congruence\ modulo$ 4".
Let $\bar{a}$ denote the equivalence class of the integer a. Then

$$\bar{a} = \{x \in \mathbb{Z} | x \equiv a\ (mod 4)\} = \{x | x - a = 4k, for\ some\ integer\ k\} = \{x = a + 4k | k \in \mathbb{Z}\}$$

Which gives, $\bar{0} = \{x = 0 + 4k | k \in \mathbb{Z}\} = \{\dots, -8, -4, 0, 4, 8, \dots\}$
$\bar{1} = \{x = 1 + 4k | k \in \mathbb{Z}\} = \{\dots, -7, -3, 1, 5, 9, \dots\}$
$\bar{2} = \{x = 2 + 4k | k \in \mathbb{Z}\} = \{\dots, -6, -2, 2, 6, 10, \dots\}$
$\bar{3} = \{x = 3 + 4k | k \in \mathbb{Z}\} = \{\dots, -5, -1, 3, 7, 11, \dots\}$.

Thus, $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ is a partition of $(\mathbb{Z}, +)$ by the relation "$congruence\ modulo$ 4".
Hence, it is the quotient structure of $(\mathbb{Z}, +)$ given by the relation "$congruence\ modulo$ 4".
It is generally denoted $\mathbb{Z}_4$.
$i.e. \mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$.
In general, $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$ is the quotient structure of $(\mathbb{Z}, +)$ given by the relation "$congruence\ modulo\ n$", where each $\bar{a} \in \mathbb{Z}_n$ represents the equivalence class of $a \in \mathbb{Z}$.

Note:
Let $(G,*)$ be an algebraic structure and R be an equivalence relation on it. For any two equivalence classes $[a], [b]$, $[a] * [b] = \{x \in \mathbb{Z} \mid x\ is\ equivalent\ to\ (a * b)\} = [a * b]$.

Note:

- Consider a binary operation $+_n$ on $\mathbb{Z}_n$,known as "$+\ modulo\ n$" defined as
  $\bar{a} +_n \bar{b} = \{x \in \mathbb{Z} \mid x\ is\ equivalent\ to\ (a + b)\} = \overline{a + b} = \bar{k}$, for some $0 \le k \le n - 1$
  Thus, for $\bar{a}, \bar{b} \in \mathbb{Z}_n$, $\bar{a} +_n \bar{b} = \bar{k}$, if $a + b \equiv k(mod\ m)$ for some $0 \le k \le n - 1$
- The members of the set $\mathbb{Z}_n = \{0,1,2, \dots, n-1\}$ are also called residue classes modulo n.

Problem.1. Prove that $(\mathbb{Z}_m, +_m)$ is an abelian group, where $\bar{a}+_m\bar{b} = \bar{k}$ if $a + b \equiv k(mod\ m)$, for some $0 \leq k \leq m-1$.

Solution.

(i)	Closure property:	For any $\bar{a}, \bar{b} \in \mathbb{Z}_m$; if $a + b \equiv k(mod\ m)$ with $0 \leq k \leq m-1$then $\bar{a}+_m\bar{b} = \bar{k}$ and it belongs to $\mathbb{Z}_m$ because $0 \leq k \leq m-1$. Hence, $\mathbb{Z}_m$ is closed under the operation $+_m$
(ii)	Associativity:	Clearly, associativity of $+_m$ depends of associativity of $+$, and we know that $+$ is associative on $\mathbb{Z}$. Therefore, $+_m$ is associative on $\mathbb{Z}_m$.
(iii)	Identity Element:	For $\bar{0} \in \mathbb{Z}_m$, and for any $\bar{a} \in \mathbb{Z}_m$, $a + 0 \equiv k(mod\ m)$ gives $\bar{a}+_m\bar{0} = \bar{a}$ and $0 + a \equiv k(mod\ m)$ gives $\bar{0}+_m\bar{a} = \bar{a}$. Hence, $\bar{0}$ is the identity element in $\mathbb{Z}_m$.
(iv)	Inverse element:	For $\bar{a} \in \mathbb{Z}_m$, $\overline{m-a} \in \mathbb{Z}_m$, for $0 \leq a \leq m-1$. Further,$\bar{a}+_m\overline{(m-a)} = \bar{0}$ because $a + (m-a) = m \equiv 0(mod\ m)$ Similarly, $\overline{(m-a)}+_m\bar{a} = \bar{0}$ Thus, $\overline{(m-a)}$ the inverse element of $[a]$ in $\mathbb{Z}_m$.
(v)	Commutative property:	For any $\bar{a}, \bar{b} \in \mathbb{Z}_m$; let $a + b \equiv k(mod\ m)$ for some $0 \leq k \leq m-1$ then $\bar{a}+_n\bar{b} = k$ Also, $b + a \equiv k(mod\ m) \Longrightarrow \bar{b}+_m\bar{a} = k$. Therefore $\bar{a}+_n\bar{b} = \bar{b}+_m\bar{a}$ Hence, $+_m$ is commutative on $\mathbb{Z}_m$.

Thus $(\mathbb{Z}_m, +_m)$ is an abelian group.

Problem.2. Prove that $\mathbb{Z}_3$ is an abelian group under the addition modulo 3.

Solution.

Consider the set $\mathbb{Z}_3 = \{0,1,2\}$.

In the following table, each cell denotes the product of the corresponding elements under the given operation.

$+_3$	**0**	**1**	**2**
0	0	1	2
1	1	2	0
2	2	0	1

From the table, closure property and associative property are obvious.

Further, symmetricity about the diagonal shows the commutative property.

Also, 0 is the identity element.

Also, the cell containing 0 gives the pair of inverse elements. And every element has an inverse.

Hence, $(\mathbb{Z}_3, +_3)$ is an abelian group.

all the properties of abelian group can be verified. Hence, it is an abelian group.

Problem.3. Let the multiplication modulo n be defined as $\bar{a} \cdot_n \bar{b} = \bar{k}$, if $ab \equiv k(mod\ n)$ for some $0 \leq k \leq n-1$. Check if $\mathbb{Z}_4^* = \{\bar{1}, \bar{2}, \bar{3}\}$ is an abelian group under the multiplication modulo 4.

Solution. Consider the set $\mathbb{Z}_4^* = \{\bar{1}, \bar{2}, \bar{3}\}$.

For $\bar{2} \in \mathbb{Z}_4^*$, $2 \times 2 = 4 \equiv 0(mod\ 4)$. Therefore, $2 \cdot_4 2 = 0$ which does not belong to $\mathbb{Z}_4^*$.

Hence, $\mathbb{Z}_4^*$ is not closed under multiplication modulo 4 and hence it is not a group.

Problem.4

Prove that $(\mathbb{Z}_5^*, \cdot_5)$ is an abelian group.

Solution:

Consider the set $\mathbb{Z}_5^* = \{1,2,3,4\}$.

In the following table, each cell denotes the product of the corresponding elements under the given operation.

$\cdot_5$	**1**	**2**	**3**	**4**
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

From the table, closure property and associative property are obvious.

Further, symmetricity about the diagonal shows the commutative property.

Also, 1 is the identity element.

Also, the cell containing 1 gives the pair of inverse elements. And every element has an inverse.

Hence, $(\mathbb{Z}_5^*, \cdot_5)$ is an abelian group.

Problem.5

Inverse of 2 in $(\mathbb{Z}_5, +_5)$ is_____. **[Winter_2022-23]**

Problem.6

Prove that $(\mathbb{Z}_5^*, \cdot_5)$ is an abelian group. **[Winter_2019-20]**

Exercise:

1. Prove that $(\mathbb{Z}_4, +_4)$ is an abelian group.
2. Prove that $(\mathbb{Z}_3^*, \cdot_3)$ is an abelian group.

PERMUTATION GROUPS

Definition:
Permutation on a set A is a bijective function from A to A.
The set of all permutation on A is denoted by S_A. It forms a group under the operation of composition of functions. This group is known as symmetric group on A.

Symmetric group :

Let $A = \{1,2,\dots,n\}$. The corresponding symmetric group is denoted by S_n, it is known as the symmetric group on n
Thus, S_n is the set of all bijective functions from the set $\{1,2,\dots,n\}$ on to itself.
An element $\sigma \in S_n$ is written as $\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$.

For example, consider $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 1 & 4 \end{pmatrix} \in S_5$

Then. $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 5, \sigma(4) = 1, \sigma(5) = 4$.

This gives $\sigma^{-1}(2) = 1, \sigma^{-1}(3) = 2, \sigma^{-1}(5) = 3, \sigma^{-1}(1) = 4, \sigma^{-1}(4) = 5$

$\therefore \sigma^{-1}$ can be written as $\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 5 & 3 \end{pmatrix}$.

Further, if $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 5 & 3 \end{pmatrix} \in S_5$ then the products $\tau\sigma$ can be obtained as the following:

$$\tau\sigma(1) = \tau\big(\sigma(1)\big) = \tau(2) = 4; \tau\sigma(2) = \tau\big(\sigma(2)\big) = \tau(3) = 2; \text{and so on}$$

Which gives

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 5 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 1 & 5 \end{pmatrix}$$

Similarly,

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 1 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 5 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$$

Thus, $\sigma\tau$ need not be equal to $\tau\sigma$.

Hence, S_5 (and in general S_n, for $n > 2$) is not a commutative group.

Note: S_n is a finite group of order $\boldsymbol{n}!$.

Definition:
An element $\sigma \in S_n$ is called a cycle of order r if there exist symbols (numbers) $x_1, x_2, \dots x_r$ such that $\sigma(x_1) = x_2, \sigma(x_2) = x_3, \dots, \sigma(x_{r-1}) = x_r, \sigma(x_r) = x_1$ and $\sigma(x) = x$ for all symbols other than $x_1, x_2, \dots x_r$.
This cycle is denoted by $(x_1, x_2, x_3, \dots, x_r)$. It is a cycle of length r. Further the order of a cycle of length r is r.
For example, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix}$ in S_5 can be represented as a cycle of length 3 as $(2 \quad 4 \quad 5)$.
Further, $(2 \quad 4 \quad 5)^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$ which shows that the order of $(2 \quad 4 \quad 5)$ is 3.

Definition:
A transposition is a permutation that swaps two elements and leaves everything else fixed.
$i.e.$ A cycle of length 2 is called a transposition.
Note: Every permutation $\sigma \in S_n$ can be expressed as a product of disjoint cycles.

For example, $\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 4 & 5 & 1 & 3\end{pmatrix} = (1 \quad 2 \quad 4)(3 \quad 5)$

Problem.1 Write the following in permutation form

(i)$(2 \quad 3 \quad 4 \quad 6)$ in S_7 (ii) $(2 \quad 3 \quad 5)(4 \quad 7)$ in s_7

Problem.2 Find the inverse of the cycle $(4 \quad 6 \quad 2 \quad 7 \quad 3)$

Solution. $(4 \quad 6 \quad 2 \quad 7 \quad 3)^{-1} = (3 \quad 7 \quad 2 \quad 6 \quad 4)$

Problem.3 Find the inverse of the cycle $(1 \quad 2 \quad 5 \quad 3 \quad 4)$ **[Summer_2023-24]**

Problem.4. Solve the equation for x: $(1 \quad 4 \quad 2)^2 \, x = (2 \quad 3 \quad 4)^{-1}$

Solution.

$\boldsymbol{(1 \quad 4 \quad 2)^2 = (1 \quad 2 \quad 4)}$ **and** $\boldsymbol{(2 \quad 3 \quad 4)^{-1} = (4 \quad 3 \quad 2)}$

$\boldsymbol{\therefore (1 \quad 4 \quad 2)^2 \, x = (2 \quad 3 \quad 4)^{-1} \Rightarrow \quad (1 \quad 2 \quad 4)x = (4 \quad 3 \quad 2)}$

$\boldsymbol{\Rightarrow (1 \quad 2 \quad 4)^{-1}(1 \quad 2 \quad 4)x = (1 \quad 2 \quad 4)^{-1}(4 \quad 3 \quad 2)}$

$\boldsymbol{\Rightarrow \quad x = (1 \quad 2 \quad 4)^{-1}(4 \quad 3 \quad 2)}$

$\boldsymbol{\Rightarrow \quad x = (4 \quad 2 \quad 1)(4 \quad 3 \quad 2)}$

$\boldsymbol{\Rightarrow \quad x = (1 \quad 4 \quad 3)}$

Problem.5

$\tau = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 4 & 2 & 5 & 3\end{pmatrix}, \sigma = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 3 & 5 & 1 & 4\end{pmatrix}$, Find τσ and στ **[Summer_2023-24]**

Que 1.) What is the Order of the Group S_4 **[Summer_2018-19]**

Que 2.) Consider the following elements of s_5 **[Summer_2018-19, Winter_2017-18]**

$$\alpha = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 3 & 1 & 4 & 5\end{pmatrix}, \quad \beta = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 2 & 3 & 5 & 4\end{pmatrix},$$
$$\gamma = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 5 & 4 & 3 & 1 & 2\end{pmatrix}, \quad \delta = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 3 & 2 & 1 & 5 & 4\end{pmatrix}$$

i.) Find $\alpha\beta\delta\gamma\,, \alpha\gamma\delta\beta, \alpha\beta\gamma\delta$
ii.) Find γ^{-1}
iii.) Find the Order of α
iv.) Solve hr equation $\delta x = \beta$
v.) What is the order of s_5

Note: Every permutation is a product of transpositions.
For example $(1 \quad 2 \quad 3 \quad \dots \quad n) = (1 \quad n) \dots (1 \quad 3)(1 \quad 2)$

Note: Expression of a permutation as a product of transpositions is not unique.

For example, $(2 \quad 7 \quad 4 \quad 5) = (2 \quad 5)(2 \quad 4)(2 \quad 7)$

And $(2 \quad 7 \quad 4 \quad 5) = (2 \quad 5)(2 \quad 4)(2 \quad 7)(3 \quad 6)(3 \quad 6)$

Definition:

A permutation is even if it can be written as a product of an even number of transpositions; a permutation is odd if it can be written as a product of an odd number of transpositions.

Note:

- A cycle of length n is odd if n is even, and it is even if n is odd.
- The set A_n of all even permutations forms a group under function composition. Hence, it is a subgroup of S_n

Problem.1.

Check if the following permutations are even or odd.

(i) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 7 & 4 & 1 & 5 & 3 & 6 \end{pmatrix}$

(ii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 7 & 4 & 6 & 5 & 3 & 1 \end{pmatrix}$

Solution:

(i) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 7 & 4 & 3 & 5 & 1 & 6 \end{pmatrix} = (1 \quad 2 \quad 7 \quad 6)(3 \quad 4) = (1 \quad 6)(1 \quad 7)(1 \quad 2)(3 \quad 4)$
Since, it is a product of 4 transpositions, it is an even permutation.

(ii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 7 & 3 & 4 & 5 & 1 & 6 \end{pmatrix} = (1 \quad 2 \quad 7 \quad 6) = (1 \quad 6)(1 \quad 7)(1 \quad 2)$
Since, it is a product of 3 transpositions, it is an odd permutation.

Problem.2

Let $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 5 & 3 \end{pmatrix}, \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 1 & 4 \end{pmatrix}$, Then check whether τ and σ are

i.)commutative ii.) even or odd. **[Winter_2019-20]**

SUBGROUPS

Substructure: Let $(S,*)$ be an algebraic structure and let $S_1 \subseteq S$ such that $(S_1,*)$ is also an algebraic structure. Then S_1 is called a substructure of S.

Subgroup:
Let $(G,*)$ be a group with the identity element e and $H \subseteq G$.
H is called a subgroup of G if (i) for every $a, b \in H, ab \in H$
(ii) $e \in H$
(iii) for every $a \in H$ its inverse a^{-1} in G also belongs to H.

Notes:
- $\boldsymbol{H \leq G}$ denotes that H is a subgroup of G.
- A non-empty subset H of a group G is a subgroup if and only if $ab^{-1} \in H$ for every $a, b \in H$**.**
- A non-empty subset H of a group $(G,*)$ is a subgroup if and only if If $(H,*)$ is also a group.
- For any group G, G is a subgroup of G. Any other subgroup is called a proper subgroup of G.
- $\boldsymbol{H < G}$ denotes that H is a proper subgroup of G.
- For any group G, $\{e\}$ is a subgroup of G. Any other subgroup is called non-trivial subgroup of G.

Problem.1.
Show that set $2\mathbb{Z}$ of all even integers is a subgroup of $(\mathbb{Z},+)$.
Solution:
Let $2k, 2l$ be any two even integers with $k, l \in \mathbb{Z}$.
Then $-2l = 2(-l)$ also belongs to $2\mathbb{Z}$.
Further, $2k + (-2l) = 2k + 2(-l) = 2\big(k + (-l)\big) = 2(k - l) \in 2\mathbb{Z}$ for $k - l \in \mathbb{Z}$.
Hence, $2\mathbb{Z}$ is a subgroup of $(\mathbb{Z},+)$.

Problem.2. Let G be a group and $a \in G$. Then prove that $H = \{a^n | n \in \mathbb{Z}\}$ is a subgroup of G. Futher it is the smallest subgroup of G containing a.
Solution:
Let $x, y \in H$.
Then $x = a^n, y = a^m$ for some $m, n \in \mathbb{Z}$.
$xy^{-1} = (a^n)(a^m)^{-1} = a^n(a^{-1})^m = a^n a^{-m} = a^{n-m} \in H$ because $n - m \in \mathbb{Z}$.
Hence, H is a subgroup of G
Now, let K be a subgroup of G and $a \in K$.
Then, clearly $a^n \in K$ for all $n \in \mathbb{Z}$.
Thus $H \subseteq K$.
$i.e.$ H is the smallest subgroup of G containing a.

Exercise:
1. Prove that $\mathbb{Z}$ is a subgroup of $(\mathbb{R},+)$.
2. Prove that $3\mathbb{Z}$ is a subgroup of $(\mathbb{Z},+)$.

NORMAL SUBGROUPS

Let G be a group and A and B be any two subsets of G. Then

(i) $AB = \{ab | a \in A, b \in B\}$
(ii) $A^{-1} = \{a^{-1} | a \in A\}$
(iii) $aB = \{ab | b \in B\}$ for any $a \in G$.
(iv) $Ab = \{ab | a \in A\}$ for any $b \in G$.

Definition:
Let G be a group and H be a subgroup of G. For any $a \in G$, aH is called a left coset of H in G.
And Ha is called a right coset of H in G.
For example,

- Consider the group $(\mathbb{Z}, +)$ and its subgroup $H = 3\mathbb{Z}$.
  Then the left coset $1 + H = 1 + 3\mathbb{Z} = 1 + \{3x | x \in \mathbb{Z}\} = \{1 + 3x | x \in \mathbb{Z}\}$
  The right coset $H + 1 = 3\mathbb{Z} + 1 = \{3x | x \in \mathbb{Z}\} + 1 = \{3x + 1 | x \in \mathbb{Z}\}$
  Clearly, $1 + H = H + 1$
- Consider $G = S_3$. Denote $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.
  Then $\alpha^2 = e = \beta^2$ and the six elements can be written as $G = \{e, \alpha, \beta, \beta^2, \alpha\beta, \beta\alpha\}$.
  $H = \{e, \alpha\}$ is a subgroup of G.
  Then left coset $\beta H = \{\beta, \beta\alpha\}$ and right coset $H\beta = \{\beta, \alpha\beta\}$.
  Here, $\beta H \neq H\beta$

Definition:
A subgroup H of a group G is said to be normal in G if $xax^{-1} \in H$ for all $a \in H$, $x \in G$. It is denoted by $H \trianglelefteq G$.

Note:

- A subgroup H of a group G is said to be normal in G if and only if $xH = Hx$ for all $x \in G$.
- $H \triangleleft G$ denotes that H is a proper normal subgroup of G.

Exercise:

1. Prove that $2\mathbb{Z}$ is a normal subgroup of $(\mathbb{Z}, +)$.

CYCLIC GROUPS

Definition:
A group G is called cyclic if there exists an element $g \in G$, such that $G = \{g^n \mid n \in \mathbb{Z}\}$. G is then denoted by (g) or $< g >$. Such an element g is called the generator of G.

Note:
- A cyclic group can have more than one generators. For example, $\mathbb{Z} = (1) = (-1)$.

Problem.1.
Prove that $G = \{1, -1, i, -i\}$ is a cyclic group. What are the generators of it ? **[Winter_2021-22]**
Solution.
We know that $G = \{1, -1, i, -i\}$ is a group.
Clearly, $1 = i^4, -1 = i^2, i = i^1, -i = i^3$. Hence, $g = (i)$
Similarly, $1 = (-i)^4, -1 = (-i)^2, i = (-i)^3, -i = (-i)^1$. Hence, $g = (-i)$

Exercise:
- Prove that $G = \left\{\ldots, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, 16, \ldots\right\}$ is a cyclic group with Usual Multiplication and generator $\frac{1}{2}$.
- Prove that $\mathbb{Z}_n$ with addition modulo n is cyclic.

Theorem
If G is a cyclic group then G is abelian.
Proof
Let $G = (a)$ and let $x, y \in G$.
Then $x = a^m, y = a^n$ for some integers m, n
Now, $xy = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m = yx$
Hence, G is abelian.

Note:
- Any subgroup of a cyclic group is cyclic.

Definition:
If G is a group with the identity element e. Let $a \in G$.
Len n be the smallest positive integer such that $a^n = e$. Then n is called the order a.
If no such n exists then order of a is defined to be infinite.
It is denoted by $o(a)$.

Problem.1.
Find the order of i in $\mathbb{C}^*$ under the multiplication. **[Winter_2022-23]**
Solution:
1 is the identity element.
Further, $i^1 = i \neq 1$, $i^2 = -1 \neq 1$, $i^3 = -i \neq 1$, $i^4 = 1$.
$i.e.$ 4 is the smallest positive integer such that $i^4 = 1$. Hence, $o(i) = 4$

Problem.2
If G={-1,1} order of (-1) is _____. **[Winter_2022-23]**

Problem.3
If $G = \{a, a^2, a^3, a^4, a^5, a^6 = e\}$ is a Group under Multiplication, then Find the order of the all the element of G. **[Summer_2018-19, Winter_2017-18, Winter_2021-22]**

Exercise:

1. Find the order of $\overline{3}$ in $\mathbb{Z}_5$ and $\mathbb{Z}_6$.
2. S_3 is cyclic ? Justify your ans.

GROUP HOMOMORPHISM & GROUP ISOMORPHISM

Group Homomorphism:

Let $(G,*)$ and $(G',\cdot)$ be two groups. A function $f: G \to G'$ is said to be a group homomorphism if $f(a * b) = f(a) \cdot f(b)$, for every $a, b \in G$.

Group Isomorphism:

Let $(G,*)$ and $(G',\cdot)$ be two groups. A bijective homomorphism $f: G \to G'$ is said to be a group isomorphism.

Note:

- If $f: G \to G'$ is an onto group homomorphism and if G is abelian then G' is also abelian. $i.e.$ An onto homorphism maps an abelian group to an abelian group.
- If $f: G \to G'$ is an onto group homomorphism and if G is cyclic then G' is also cyclic. $i.e.$ An onto homorphism maps a cyclic group to a cyclic group.
- If $f: G \to G'$ is a group homomorphism then (i) $f(e) = e'$ and (ii)$f(a^{-1}) = \big(f(a)\big)^{-1}$ $i.e.$ A group homomorphism maps identity to identity and inverse of an image is image of the inverse.
- If $f: G \to G'$ is a group homomorphism then the set $ker(f) = \{a \in G | f(a) = e'\}$ is a normal subgroup of G. It is known as kernel of f.

Problem.1.
Prove that $G' = \{1, -1\}$ forms a group under the multiplication.
Also prove that $f: \mathbb{Z} \to G'$ defined as $f(a) = 1$ if a is even, otherwise $f(a) = -1$,is a group homomorphism.
Solution:
Clearly, multiplication is closed and associative on G'. Further 1 is the identity element. And both elements are self-inverse. Hence, $G' = \{1, -1\}$ forms a group under the multiplication.
Let m, n be any integers such that $mn \geq 0$.
If both m and n are even then $m + n$ is also even.
Further, $f(m) = f(n) = 1$ and $f(m + n) = 1 = f(m)f(n)$
If both m and n are odd then $m + n$ is even.
Further, $f(m) = f(n) = -1$ and $f(m + n) = 1 = (-1)(-1) = f(m)f(n)$
If one of them (say m) is odd and other $(say\ n)$ is even then $m + n$ is odd.
Further, $f(m) = -1, f(n) = 1$and $f(m + n) = -1 = (-1)(1) = f(m)f(n)$
Thus, in any case, $f(m + n) = f(m)f(n)$.
Hence, f is a group homomorphism.

Problem.2.
Let $\mathbb{R}^+$ be the group of positive real numbers under multiplication. Let $f: \mathbb{R} \to \mathbb{R}^+$ be defined as $f(a) = 2^a$, for all $a \in \mathbb{R}$. Then prove that f is a group homomorphism.
Solution
For any , $b \in \mathbb{R}$,$f(a + b) = 2^{a+b} = 2^a 2^b = f(a)f(b)$.
Hence, proved.

RINGS

Definition:
A ring $(R, +, \cdot)$ is a non-empty set R with two binary operations denoted by $+$ and $\cdot$ subject to the following conditions:
(i) $(R, +)$ is an abelian group.
(ii) $(R, \cdot)$ is a semi-group.
(iii) $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$
$i.e.$ $\cdot$ is distributive over $+$.

Definition:
A ring $(R, +, \cdot)$ is said to be a ring with unit element (identity) if there exists an element $e \in R$ such that $e \cdot a = a \cdot e = a$ for every $a \in R$.

Definition:
A ring $(R, +, \cdot)$ is said to be a commutative if $a \cdot b = b \cdot a$ for every $a, b \in R$.

Note:
- In a ring $(R, +, \cdot)$ the identity element under $+$ is known as a zero element. Similarly, unit element is the identity element under the second operation.

Problem.1. Prove that $R = 2\mathbb{Z}$ is a ring under usual addition and multiplication.

Problem.2. Prove that $R = \mathbb{R}$ is a ring under usual addition and multiplication.

Problem.3. Prove that $R = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \text{ are real numbers} \right\}$ with usual matrix addition is an abelian group. Let the matrix multiplication be distributive over addition to make it a ring. Find the unit element of this ring. Is it a commutative ring? **[Winter_2019-20]**

Integral Domain

Definition:

Let R be a ring. Then $a \in R$ $(\neq 0)$ is called a zero divisor of R if there exists $b \in R$ $(\neq 0)$ such that $a.b = 0$.

Definition:

A commutative ring which has no zero divisor is called an integral domain.

Problem.1. Prove that the ring of 2×2 real matrices is not an integral domain.
Solution:
We know that $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ is the zero element of the ring.
Consider, $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ then $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.
Hence, $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ are zero divisors in the ring. Hence, it is not an integral domain.

Problem.2. Check if $R = 2\mathbb{Z}$ is an integral domain under usual addition and multiplication.

Problem.3. Prove that $R = \mathbb{R}$ is an integral domain under usual addition and multiplication
.

Problem.4. Prove that $R = \mathbb{Z}_5$ is an integral domain under addition and multiplication modulo 5.

Problem.5. Check if $R = \mathbb{Z}_4$ is an integral domain under addition and multiplication modulo 5.

Problem.6. A commutative ring which has no zero divisor is called ____ **[Winter_2019-20]**

FIELDS

Definition:
A commutative ring R with unit element $1 \neq 0$ in which every non-zero element has an inverse with respect to multiplication is called a **field.**

Definition:
A ring R with unit element $1 \neq 0$ in which every non-zero element has an inverse with respect to multiplication is called a **skew-field.**
Note:
By definition, every field is a skew-field.

Problem.1.
Prove that ring of real numbers is a field.

Problem.2.
Prove that ring of rational numbers is a field

Problem.3.
Prove that $\mathbb{Z}_3$ is a field.

BOOLEAN ALGEBRA

Boolean algebra provides the operations and the rules for working with the set $\{0, 1\}$.
Electronic and optical switches can be studied using this set and the rules of Boolean algebra.

Operations in Boolean algebra:

Operation	Notation	Definition (Result)
Complementation	$\bar{a}$	$\bar{0} = 1$ and $\bar{1} = 0$
Boolean sum	$+$ or OR	$1 + 1 = 1 \quad 1 + 0 = 1$ $0 + 1 = 1 \quad 0 + 0 = 0$
Boolean product	$\cdot$ or AND	$1 \cdot 1 = 1 \quad 1 \cdot 0 = 0$ $0 \cdot 1 = 0 \quad 0 \cdot 0 = 0$

Note:

- When there is no danger of confusion, the symbol $\cdot$ can be deleted, just as in writing algebraic products.
- Unless parentheses are used, the rules of precedence for Boolean operators are: first all complements are computed, followed by all Boolean products, followed by all Boolean sums.
- The complement, Boolean sum, and Boolean product correspond to the logical operators, ¬,∨, and ∧, respectively, where 0 corresponds to **F** (false) and 1 corresponds to**T** (true).
- Equalities in Boolean algebra can be directly translated into equivalences of compound propositions. Conversely, equivalences of compound propositions can be translated into equalities in Boolean algebra

Problem.1. Find the value of the following.

(i) $1 \cdot 0 + \overline{(0 + 1)}$ (ii) $1 + 0 \cdot \overline{0 + 1 \cdot 0}$

Problem.2. Translate **the following** into a logical equivalence.

(i) $1 \cdot 0 + \overline{(0 + 1)}$ (ii) $1 + 0 \cdot \overline{0 + 1 \cdot 0}$

Problem.3. Translate the logical equivalence $(\mathbf{T} \wedge \mathbf{T}) \vee \neg \mathbf{F} \equiv \mathbf{T}$ into an identity in Boolean algebra.

Solution: $1 \cdot 1 + \bar{0} = 1$

Boolean Expression and Boolean Function

Let $B = \{0, 1\}$. Then $B^n = \{(x_1, x_2, \ldots, x_n) x_i \in B \; for \; 1 \leq i \leq n\}$ is the set of all possible $n - tuples$ of $0s$ and $1s$.

The variable x is called a **Boolean variable** if it assumes values only from B, that is, if its only possible values are 0 and 1.

A function from $B^n \; to \; B$ is called a **Boolean function of degree *n***.

Boolean functions can be represented using expressions made up from variables and Boolean operations.

If E_1 and E_2 are Boolean expressions, then E_1, $(E_1 E_2)$, and $(E_1 + E_2)$ are Boolean expressions.

Each Boolean expression represents a Boolean function.

The values of this function are obtained by substituting 0 and 1 for the variables in the expression.

Problem.1. Find the values of the Boolean function represented by $F(x, y, z) = xy + \bar{z}$
Solution. The values of this function are displayed in the following table.

x	y	z	xy	$\bar{z}$	$F(x, y, z) = xy + z$
1	1	1	1	0	1
1	1	0	1	1	1
1	0	1	0	0	0
1	0	0	0	1	1
0	1	1	0	0	0
0	1	0	0	1	1
0	0	1	0	0	0
0	0	0	0	1	1

Boolean functions F and G of n variables are equal if and only if $F(x_1, x_2, \ldots, x_n) = G(x_1, x_2, \ldots, x_n)$ whenever $x_1, x_2, \ldots, x_n$ belong to B.
Two different Boolean expressions that represent the same function are called **equivalent**.
For instance, the Boolean expressions xy, $xy + 0$, and $xy \cdot 1$ are equivalent.
The **complement** of the Boolean function F is the function $\bar{F}$, where

$$\bar{F}(x_1, x_2, \ldots, x_n) = \overline{F(x_1, x_2, \ldots, x_n)}$$

Let F and G be Boolean functions of degree n. The **Boolean sum** $F + G$ and the **Boolean product** FG are defined by

$$(F + G)(x_1, x_2, \ldots, x_n) = F(x_1, x_2, \ldots, x_n) + G(x_1, x_2, \ldots, x_n),$$
$$(FG)(x_1, x_2, \ldots, x_n) = F(x_1, x_2, \ldots, x_n)G(x_1, x_2, \ldots, x_n).$$

Problem.1. How many different Boolean functions of degree *n* are there?
Solution: From the product rule for counting, it follows that there are 2^n different $n - tuples$ of $0s\ and\ 1s$. Because a Boolean function is an assignment of $0\ or\ 1$ to each of these 2^n different $n - tuples$, the product rule shows that there are 2^{2^n} different Boolean functions of degree n.

Identities of Boolean Algebra

There are many identities in Boolean algebra. The most important of these are displayed the following table. These identities are particularly useful in simplifying the design of circuits. Each of the identities in table below can be proved using a table.

Identity	*Name*
$\overline{\overline{x}} = x$	Law of the double complement
$x + x = x$ $x \cdot x = x$	Idempotent laws
$x + 0 = x$ $x \cdot 1 = x$	Identity laws
$x + 1 = 1$ $x \cdot 0 = 0$	Domination laws
$x + y = y + x$ $xy = yx$	Commutative laws
$x + (y + z) = (x + y) + z$ $x(yz) = (xy)z$	Associative laws
$x + yz = (x + y)(x + z)$ $x(y + z) = xy + xz$	Distributive laws
$\overline{(xy)} = \overline{x} + \overline{y}$ $\overline{(x + y)} = \overline{x}\,\overline{y}$	De Morgan's laws
$x + xy = x$ $x(x + y) = x$	Absorption laws
$x + \overline{x} = 1$	Unit property
$x\overline{x} = 0$	Zero property

Problem.1. Prove that $x(y + z) = xy + xz$

Solution.

x	y	z	$y + z$	$x(y + z)$	xy	xz	$xy + xz$
1	1	1	1	1	1	1	1
1	1	0	1	1	1	0	1
1	0	1	1	1	0	1	1
1	0	0	0	0	0	0	0
0	1	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	0	1	1	0	0	0	0
0	0	0	0	0	0	0	0

Since, both the expressions have same values they are same(equivalent).

Exercise: Prove the associative law for Boolean sum.

Duality

The dual of Boolean expression is obtained by interchanging Boolean Sums and Boolean Products, and interchanging $0s$ and $1s$.
For example, the dual of $x \cdot (y + 0)$ is $x + (y \cdot 1)$ and the dual of $x \cdot 1 + (\bar{y} + z)$ is $(x + 0) \cdot (\bar{y} \cdot z)$

Disjunctive Normal Form

Definition.
A **literal** is a Boolean variable or its complement.
A *minterm* of the Boolean variables $x_1, x_2, \ldots, x_n$ is a Boolean product $y_1 y_2 \ldots y_n$ where $y_i = x_i \; or \; y_i = \bar{x}_i$. Hence, a **minterm** is a Boolean product of **n** literals, with one literal for each variable.
A minterm is the standard product.

Note:
A minterm has the value 1 for one and only one combination of values of its variables.
More precisely, the minterm $y_1 y_2 \ldots y_n$ is 1 if and only if each y_i is 1, and this occurs if and only if $x_i = 1$ when $y_i = x_i$ and $x_i = 0$ when $y_i = \bar{x}_i$.

Problem.1. Find a minterm that equals 1 if $x_1 = x_3 = 0$ and $x_2 = x_4 = x_5 = 1$, and equals 0 otherwise.
Solution. The minterm $\overline{x_1} x_2 \overline{x_3} x_4 x_5$ has the correct set of values.

By taking Boolean sums of distinct minterms we can build up a Boolean expression with a specified set of values. In particular, a Boolean sum of minterms has the value 1 when exactly one of the minterms in the sum has the value 1.
It has the value 0 for all other combinations of values of the variables.
Consequently, given a Boolean function, a Boolean sum of minterms can be formed that has the value 1 when this Boolean function has the value 1, and has the value 0 when the function has the value 0.
The minterms in this Boolean sum correspond to those combinations of values for which the function has the value 1.

Definition.
The sum of minterms that represents the function is called the **sum-of-products expansion** or the **disjunctive normal form** of the Boolean function.

Problem.1. Find the sum-of-products expansion for the function $F(x, y, z) = (x + y)\bar{z}$ using the Boolean identities.
Solution.

$$
\begin{aligned}
F(x, y, z) &= (x + y)\bar{z} \\
&= x\bar{z} + y\bar{z} && \text{Distributive law} \\
&= x1\bar{z} + 1y\bar{z} && \text{Identity law} \\
&= x(y + \bar{y})\bar{z} + (x + \bar{x})y\bar{z} && \text{Unit property} \\
&= xy\bar{z} + x\bar{y}\bar{z} + xy\bar{z} + \bar{x}y\bar{z} && \text{Distributive law} \\
&= xy\bar{z} + x\bar{y}\bar{z} + \bar{x}y\bar{z} && \text{Idempotent law}
\end{aligned}
$$

Problem.2. Find the sum-of-products expansion for the function $F(x, y, z) = (x + y)\bar{z}$ using the table of values.

Solution.

Consider the following table of values of the function $F(x, y, z) = (x + y)\bar{z}$.

x	y	z	$x + y$	$\bar{z}$	$(x + y)\bar{z}$
1	1	1	1	0	0
1	1	0	1	1	**1**
1	0	1	1	0	0
1	0	0	1	1	**1**
0	1	1	1	0	0
0	1	0	1	1	**1**
0	0	1	0	0	0
0	0	0	0	1	0

The sum-of products expansion of F is the Boolean sum of three minterms corresponding to the three rows of this table that give the value 1 for the function. This gives

$$F(x, y, z) = xy\bar{z} + x\bar{y}\bar{z} + \bar{x}y\bar{z}$$

Conjunctive Normal Form

It is also possible to find a Boolean expression that represents a Boolean function by taking a Boolean product of Boolean sums. The resulting expansion is called the **conjunctive normal form** or **product-of-sums expansion** of the function. These expansions can be found from sum-of-products expansions by taking duals.

Problem.1. Find the product-of-sums expansion for the function $F(x, y, z) = (x + y)\bar{z}$ using the table of values. **[Winter 2019-20]**

Solution.

Consider the following table of values of the function $F(x, y, z) = (x + y)\bar{z}$.

x	y	z	$x + y$	$\bar{z}$	$(x + y)\bar{z}$
1	1	1	1	0	0
1	1	0	1	1	**1**
1	0	1	1	0	0
1	0	0	1	1	**1**
0	1	1	1	0	0
0	1	0	1	1	**1**
0	0	1	0	0	0
0	0	0	0	1	0

The sum-of products expansion of F is the Boolean sum of three minterms corresponding to the three rows of this table that give the value 1 for the function. This gives the sum-of-product expression as

$$F(x, y, z) = xy\bar{z} + x\bar{y}\bar{z} + \bar{x}y\bar{z}$$

Taking the dual of this,

$$F(x, y, z) = (x + y + \bar{z})(x + \bar{y} + \bar{z})(\bar{x} + y + \bar{z})$$

Which is the required product-of-sums expansion.

BOOLEAN RING

Let $B = \{0,1\}$. Define $x \oplus y = (x \wedge \neg y) \vee (\neg x \wedge y)$ for the ring sum of $x \; and \; y$, and use $xy = x \cdot y$ for their product. Prove that $(B, \oplus, \cdot)$ forms a ring.

Solution:

Consider the table for the ring sum on $B = \{0,1\}$.

$\oplus$	0	1
0	0	1
1	1	0

Which shows that the ring sum satisfies both the closure property and associative property.

Further 0 is the zero element. And both the elements are self-inverse.

Hence, B is a group under ring sum.

Further, Boolean product satisfies closure property.

Further $x \cdot (y \oplus z) = (x \cdot y) \oplus (x \cdot z)$ can be verified by the following table as product of both the sides are same in each case.

x	y	z	$y \oplus z$	$x \cdot (y \oplus z)$	$(x \cdot y)$	$(x \cdot z)$	$(x \cdot y) \oplus (x \cdot z)$
0	0	0	0	0	0	0	0
0	0	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	1	1	0	0	0	0	0
1	0	0	0	0	0	0	0
1	0	1	1	1	0	1	1
1	1	0	1	1	1	0	1
1	1	1	0	0	1	1	0

Thus, it forms a ring.