Date
Page No.

UNIT-4

Algebraic structure →

Definition → A Non empty Set G equipped with one or more binary operation is called an algebraic structure.
Suppose * is a binary operation on G. Then (G, *) is an algebraic structure.
(N, +), (I, +), (I, −), (R, +, ·) are all algebraic structure. Obviously addition and multiplication are both binary operations on the Set R of real Number. Therefore (R, +, ·) is an algebraic structure equipped with two operations.

BINARY OPERATION → Consider a Non empty Set A and a function f such that $f: A \times A \to A$ is called a binary operation on A. If * is a binary operation on A. then it may be written as $a * b$.
A binary operation can be denoted by any of the symbols +, −, ×, ⊕, ∘, ∨, ∧ etc.

SEMIGROUP → Let us consider an algebraic system $(A, *)$ where $*$ is a binary operation on A. Then the System $(A, *)$ is said to be a semi-group if it satisfies the following properties:

1. The operation $*$ is an closed operation on set A. i.e $a * b \in A$. where $a, b \in A$.
2. The operation $*$ is an associative operation.

i.e if $a, b, c \in A$. then

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

Example Consider an algebraic system $(A, *)$ where $A = \{1, 3, 5, 7, 9 \ldots\}$, the set of all positive odd integer and $*$ is a binary operation means multiplication Determine whether $(A, *)$ is a semi group.

Soln

closure property → The operation $*$ is a closed operation because multiplication of two +ve odd Integers is a +ve odd Number.

Associative property → The operation

Date
Page No.

* is an associative operation on set A. Since for every a, b, c ∈ A we have

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

Hence, the algebraic system $(A, *)$ is a semigroup.

Example Consider the algebraic system $(\{0,1\}, *)$ where * is a multiplication operation. Determine whether $(\{0,1\}, *)$ is a semigroup.

Soln → Closure property → The operation * is a closed one on the given set since $0*0=0$; $0*1=0$; $1*0=0$; $1*1=1$

Associative property → The operation * is a ~~closed~~ Associative. Since we have $(a*b)*c = a*(b*c)$ ∀ a, b, c

Since, the algebraic system is closed associative, Hence it is a semi-group.

Example. Let $(A, *)$ be semi group. Show that for a, b, c in A, if $a*b = c*a$ and $b*c = c*b$ then $(a*b)*c = c*(a*b)$

Page No.

Sol: Take L.H.S we have

$(a*b)*c \Rightarrow a*(b*c)$

$\because$ ($*$ is associative)

$\Rightarrow a*(c*b)$ ($\because b*c = c*b$)

$\Rightarrow (a*c)*b$ ($\because *$ is associative)

$\Rightarrow (c*a)*b$ ($\because a*c = c*a$)

$\Rightarrow c*(a*b)$ ($\because *$ is associative)

which is equal to R.H.S

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

Date.
Page No.

MONOID → Let us consider an algebraic system (A, o), where o is a binary operation on A. Then the system (A, o) is said to be a monoid if it satisfies the following properties:

(1) The operation o is a closed operation on set A.
i.e $a o b \in A, \forall a, b \in A$.

(2) The operation o is an associative operation
i.e $a o (b o c) = (a o b) o c \quad \forall a, b, c \in A$.

(3) There exist an identity element with respect to the operation o
$a o e = a \quad \forall a \in A$ where e is the identity element.

Example → Consider an algebraic system $(W, +)$ where the set $W = \{0, 1, 2, 3, 4 \ldots\}$ the set of ~~natural~~ whole Numbers and $+$ is an addition operation. Determine whether $(W, +)$ is a monoid.

Soln (1) closure property → The operation $+$ is closed since sum of two Natural

Date
Page No.

Whole
Number is a ~~Natural~~ Number

i.e $1+2=3 ; 3 \in W$

(2) Associative property → The operation + is an associative property since we have

$(a+b)+c = a+(b+c) \quad \forall a, b, c \in N$

let $a=0, b=1, c=2$

Then L.H.S $= (0+1)+2$
$= 1+2$
$= 3$

R.H.S $= a+(b+c)$
$= 0+(1+2)$
$= 0+3$
$= 3$

Hence L.H.S = R.H.S

(3.) Identity There exist an identity element in set W. with respect to the operation +. The element 0 is an identity element with respect to the operation +. Since the operation + is a closed associative and there exist an identity. Hence, the algebraic system $(W, +)$ is a monoid.

Date:
Page No.

Group → Let us consider an algebraic system $(G, *)$, where $*$ is a binary operation on G. Then the system $(G, *)$ is said to be a group if it satisfies following properties.

Closure property

(1) The operation $*$ is a closed operation
$a * b \in G \quad \forall \; a, b \in G$.

Associative property

(2) The operation $*$ is an associative operation
$a * (b * c) = (a * b) * c \quad \forall a, b, c \in G$

Identity property

(3) There exists an identity element with respect to the operation $*$
$a * e = a \quad \forall \; a \in G$ where e is the identity element.

Inverse property

(4) For every $a \in G$, there exists an element $a^{-1} \in G$ such that
$a^{-1} * a = a * a^{-1} = e \quad \forall a \in G$
where a^{-1} is Inverse of a and e is Identity element.

Example Determine whether the algebraic system $(Q, +)$ is a group where Q is the set of

Date
Page No.

all rational Numbers and + is an addition operation.

Soln →

① closure property → The set Q is closed under operation +, since the addition of two rational Numbers is a rational Number

i.e $\frac{1}{2} + \frac{1}{3} = \frac{2+3}{6} = \frac{5}{6}$ and

$\frac{1}{2}, \frac{1}{3} \in Q$ and $\frac{5}{6} \in Q$.

② Associative Property → The operation + is associative, since $(a+b)+c = a+(b+c)$ $\forall a, b, c \in Q$.

Let $a = \frac{1}{2}$, $b = \frac{1}{3}$, $c = \frac{1}{4}$

R.H.S $= \frac{1}{2} + \left(\frac{1}{3} + \frac{1}{4}\right)$

$= \frac{1}{2} + \left(\frac{4+3}{12}\right)$

$= \frac{1}{2} + \frac{7}{12} = \frac{6+7}{12} = \frac{13}{12}$ ——(1)

R.H.S $= (a+b)+c$

$= \left(\frac{1}{2} + \frac{1}{3}\right) + \frac{1}{4}$

$= \left(\frac{3+2}{6}\right) + \frac{1}{4}$

Date.
Page No.

$$\frac{5}{6} + \frac{1}{4} = \frac{5\times 2 + 1\times 3}{12} = \frac{10+3}{12}$$

$$= \frac{13}{12} \in Q$$

Hence L.H.S = R.H.S

(3) (4) Identity Property → The element 0 is the identity element. Hence

$a + 0 = 0 + a \quad \forall\ a \in Q$

$\frac{1}{2} + 0 = \frac{1}{2} \in Q$ and $0 \in Q$

where 0 is the identity element.

(4) Inverse property → The inverse of every element $a \in Q$ is $-a \in Q$. Hence the inverse of every element exist.

~~Since, the alg~~ i.e

$$\frac{1}{2} - \frac{1}{2} = 0$$

then $-\frac{1}{2}$ is inverse of $\frac{1}{2}$

Since, the algebraic system $(Q, +)$ satisfy all the property of a group Hence $(Q, +)$ is a group.

Date.
Page No.

ABELIAN GROUP → Let us consider an algebraic system $(G, *)$ where $*$ is a binary operation on G. Then the system $(G, *)$ is said to be an abelian group if it satisfies all the properties of the group plus an additional following property. The operation $*$ is commutative i.e $a * b = b * a \ \forall a, b \in G$.

Q. Consider an algebraic system $(G, *)$ where G is the set of all non-zero real numbers and $*$ is a binary operation defined by:

$$a * b = \frac{ab}{4}$$

Show that $(G, *)$ is an abelian group

Soln →

(1) closure property → The set G is closed under the operation $*$. Since $a * b = \frac{ab}{4}$ is a real Number. Hence belong to G.

(2) Associative property → The operation $*$ is associative. Let $a, b, c \in G$, then we have

$$(a*b)*c = \left(\frac{ab}{4}\right)*c = \frac{(ab)c}{16} = \frac{abc}{16}$$

Similarly

$$a*(b*c) = a*\left(\frac{bc}{4}\right) = \frac{a(bc)}{16} = \frac{abc}{16}$$

(3) Identity → To find the Identity element
Let us assume that e is a +ve real number. Then $e*a = a$.
where $a \in G$.

$$\frac{ea}{4} = a \quad \text{or} \quad e = 4$$

Thus, the identity element in G is 4.

(4) Inverse property → Let us assume that $a \in G$. If $a^{-1} \in Q$ is an inverse of a, then $a*a^{-1} = 4$.
Therefore $\frac{aa^{-1}}{4} = 4$

$$\text{or } a^{-1} = \frac{16}{a}$$

(5) Commutative property → The operation * on G is commutative
since $a*b = \frac{ab}{4} = \frac{ba}{4} = b*a$

Thus the algebraic system $(G, *)$ is

Date
Page No.

closed, associative, identity element, inverse and commutative. Hence, the system $(G, *)$ is an abelian group.

Properties of group →

Theorem 1. Uniqueness of identity

The identity element in a group is unique.

Proof → Suppose e and e' are two identity element of a group G.

We have

$ee' = e$ if e' is identity

and $ee' = e'$ if e is identity.

But ee' is unique element of G.

Therefore $ee' = e$ and $ee' = e'$

$\Rightarrow e = e'$

Hence the identity element is unique.

Date: _____
Page No. _____

Theorem 2. Uniqueness of inverse: The inverse of each element of a group is unique.

Proof → Let a be any element of a group G and let e be the identity element. Suppose b and c are two inverse of a i.e

$ba = e = ab$ and $ca = e = ac$

We have $b(ac) = be$ [$\because ac = e$]

$= b$ [$\because e$ is identity]

Also $(ba)c = ec$

$= c$ [$\because e$ is identity]

But in a group composition is Associative. Therefore $b(ac) = (ba)c$

Hence $\boxed{b = c}$

Theorem 3. If the inverse of a is a^{-1} then the inverse of a^{-1} is a i.e $(a^{-1})^{-1} = a$

Proof → If e is the identity element, we have

$a^{-1}a = e$ [By definition of inverse]

$\Rightarrow$ ~~$a^{-1}a = e$~~

$\Rightarrow (a^{-1})^{-1}[a^{-1}a] = (a^{-1})^{-1}e$ (pre multiply by $(a^{-1})^{-1}$)

Page No. _____

$\Rightarrow [(a^{-1})^{-1} a^{-1}]a = (a^{-1})^{-1}$

[$\because$ composition in G is associative and e is identity element]

$\Rightarrow ea = (a^{-1})^{-1}$

$\Rightarrow a(a^{-1})^{-1}$

$\Rightarrow (a^{-1})^{-1} = a$

SUBGROUP → A non-empty subset H of a group G is said to be a subgroup of G if the composition in G is also a composition in H and for this composition H itself.

Examples of Subgroup :

(1) The multiplicative group of positive rational Numbers is a subgroup of the multiplicative group of all non zero rational Numbers.

Date.
Page No.

(2) The additive group of even integers is a subgroup of the additive group of all integers

(3) The additive group of integers is a subgroup of the additive group of all rational numbers.

Q1. Let H be a subgroup of a group G and define $T = \{x \in G : xH = Hx\}$ prove that T is a subgroup of G.

Soln Let $x_1, x_2 \in T$. Then $x_1 H = H x_1$, $x_2 H = H x_2$

We have to show that $x_2^{-1} \in T$

We have $x_2 H = H x_2 = x_2^{-1}(x_2 H) x_2^{-1}$

$= x_2^{-1}(H x_2) x_2^{-1}$

$\Rightarrow H x_2^{-1} = x_2^{-1} H \Rightarrow x_2^{-1} \in T$.

Now we shall show that $x_1 x_2^{-1} \in T$

We have $(x_1 x_2^{-1}) H = x_1 (x_2^{-1} H) = x_1 (H x_2^{-1})$

$= (x_1 H) x_2^{-1} = (H x_1) x_2^{-1} = H (x_1 x_2^{-1})$

$\therefore x_1 x_2^{-1} \in T$.

Thus $x_1, x_2 \in T \Rightarrow x_1 x_2^{-1} \in T$. Hence T is a subgroup of G.

Q2. Show that the union of two subgroup is a subgroup if and only if one is contained in the other.

Soln → Suppose H_1 and H_2 are two subgroup of a group G. Let $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$. Then $H_1 \cup H_2 = H_2$ or H_1. But H_1, H_2 are subgroups and therefore $H_1 \cup H_2$ is also a subgroup.

Conversely, suppose $H_1 \cup H_2$ is a subgroup. To prove that $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$

Let us assume that H_1 is not a subset of H_2 and H_2 is also not a subset of H_1.

Now H_1 is not a subset of $H_2 \Rightarrow$
$\exists\ a \in H_1$ and $a \notin H_2$ — (1)
and H_2 is not a subset of $H_1 \Rightarrow$
$\exists\ b \in H_2$ and $b \notin H_1$ — (2)
from (1) and (2) we have
$a \in H_1 \cup H_2$ and $b \in H_1 \cup H_2$
since $H_1 \cup H_2$ is a subgroup, therefore $ab = c$ (say) is also an element of $H_1 \cup H_2$

But $ab = c \in H_1 \cup H_2 \Rightarrow ab = c \in H_1$ or H_2

Suppose $ab = c \in H_1$ ($\because H_1$ is a subgp

Then $b = a^{-1}c \in H_1$ ($\because a \in H_1 \Rightarrow a^{-1} \in H_1$)

But from 2 we have $b \notin H$

Again suppose $ab = c \in H_2$

Then $a = cb^{-1} \in H_2$ ($\because H_2$ is a subgroup)

Hence either $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$

Cyclic groups →

Definition → A group G is called cyclic if, for some $a \in G$, every element $x \in G$ is of the form a^n where n is some integer. Then element a is then called a generator of G.

Example The multiplicative group $G = \{1, -1, i, -i\}$ is cyclic.

We can write $G = \{i, i^2, i^3, i^4\}$.

Thus G is a cyclic group and i is a generator.

Date.
Page No.

Example The multiplicative group $\{1, \omega, \omega^2\}$ is cyclic. Then generators are ω and ω^2.

Theorem: If a is a generator of a cyclic group G, then a^{-1} is also a generator of G.

Proof: Let $G = \{a\}$ be a cyclic group generated by a. Let a^r be any element of G where r is some integer. We can write $a^r = (a^{-1})^{-r}$. Since r is also some integer, therefore each element of G is generated by a^{-1}. Thus a^{-1} is also a generator of G.

Date. _____
Page No. _____

Theorem . If finite group of order n contains an element of order n, the group must be cyclic.

proof :

Suppose G is a finite group of order n. Let $a \in G$ and let n be the order of a. If H is the cyclic subgroup of G generated by a. i.e if $H = \{a^r : r \in I\}$, then the order of H is n because the order of generator a of H is n. Thus H is cyclic subgroup of G and the order of H is equal to the order of G. Hence $H = G$. and therefore G itself is a cyclic group and a is a generator of G.

Cosets : Suppose G is a group and H is any subgroup of G. Let a be any element of G. Then the set $Ha = \{ha : h \in H\}$ is called a right coset of H in G generated by a. Similarly the set $aH = \{ah : h \in H\}$ is called a left coset of H in G generated by a.

Obviously Ha and aH are both subsets of G.

If e is the identity element of G. Therefore $e \in H$ then $He = H = eH$

Therefore H itself is a right as well as a left coset.

Example Let G be the additive group of integer i.e,

$G = \{\ldots -3, -2, -1, 0, 1, 2, 3 \ldots\}$

Let H be the subgroup of G. Obtained on multiplying each element of G by 3. Then $H = \{\ldots -9, -6, -3, 0, 3, 6, 9 \ldots\}$

Since the group G is abelian any right coset will be equal to the corresponding left coset.

Date. _____
Page No. _____

Let us form the right cosets of H in G. We have $0 \in G$ and
$H = H+0 = \{\ldots -9, -4, -3, 0, 2, 6, 9\}$
Again $1 \in G$ and $H+1 = \{\ldots -8, -5, -2, 1, 4, \ldots\}$
Then $2 \in G$ and $H+2 = \{\ldots -7, -4, -1, 2, 5, 8, 11 \ldots\}$
We see that right cosets H, $H+1$, $H+2$ are all distinct and moreover these are disjoint i.e have no element common
Now $3 \in G$ and $H+3 = H$. Also we observe that $3 \in H$.
Again $4 \in G$ and $H+4 = \{\ldots -5, -2, 1, 4, 7, 10 \ldots 13 \ldots\}$
We see that $H+4 = H+1$. Also we observe that $4 \in H+1$ similarly the right coset $H+5$ coincides with $H+2$, $H+6$ with $H+(-1)$. with $H+2$, $H+(-2)$ with $H+1$ and so on.
Thus we get only three distinct right cosets i.e H, $H+1$, $H+2$.
Obviously $G = H \cup (H+1) \cup (H+2)$.

Theorem Any two right (left) cosets of a subgroup are either disjoint or identical.

Proof :- Suppose H is a subgroup of a group G and left Ha and Hb be two right cosets of H in G. Suppose Ha and Hb are not disjoint. Then there exists at least one element say c such that $c \in Ha$ and $c \in Hb$. Let $c = h_1 a$ and $c = h_2 b$ where $h_1, h_2 \in H$

Then $h_1 a = h_2 b$

or $h_1^{-1} h_1 a = h_2^{-1} h_2 b$

or $ea = (h_2^{-1} h_2) b$

$a = (h_2^{-1} h_2) b$

Since H is a subgroup, therefore $h_1^{-1} h_2 \in H$. Let $h_1^{-1} h_2 = h_3$

Then $a = h_3 b$

Now $Ha = Hh_3 b = (Hh_3) b$

$= Hb.$

Therefore the two right cosets are identical if they are not disjoint. Thus either $Ha \cap Hb = \phi$ or $Ha = Hb$

Similarly we can prove that either $aH \cap bH = \phi$ or $aH = bH$.

Imp

Lagrange's Theorem

Statement → The order of each subgroup of a finite group is a divisor of the order of the group

proof → Let G be a group of finite order n. Let H be a subgroup of G and let o(H) = m. Suppose $h_1, h_2, \ldots h_m$ ~~are~~ are the m members of H.

Let a ∈ G. Then Ha is a right coset of H in G and we have

$Ha = \{h_1a, h_2a \ldots h_ma\}$

Ha has m distinct members, since

$h_ia = h_ja \Rightarrow h_i = h_j$

~~Ha has m distinct members~~

Therefore each right coset of H in G has m distinct members.

Any two distinct right cosets of H in G are distinct (disjoint) i.e they have no element in common.

Since G is a finite group, the Number of distinct right cosets of H in G will be finite, say equal to k. The Union of these k

Date.
Page No.

distinct right cosets of H in G is equal to G.
Thus if $Ha_1, Ha_2 \cdots Ha_k$ are the k distinct coset of H in G. then
$G = Ha_1 \cup Ha_2 \cup \cdots \cup Ha_k$
$\Rightarrow$ the Number of elements in G = the Number of elements in Ha_1 + the Number of elements in $Ha_2 + \cdots +$ the Number of elements in Ha_k

$\Rightarrow o(G) = km \Rightarrow n = km$

$\Rightarrow k = \frac{n}{m} \Rightarrow m$ is a divisor of n

$\Rightarrow o(H)$ is a divisor of $o(G)$
Hence the theorem.

Note 1 k is the Index of H in G. We have $m = \frac{n}{k}$. Thus k is a divisor of n.
Therefore the index of every subgroup of a finite group is a divisor of the order of the group.

Note 2. If H is a subgroup of a finite group G, then the.

Index of H in G = the Number of distinct right (or left) Cosets of H in G = $\frac{o(G)}{o(H)}$.

Normal Subgroup :

A subgroup H of a group G is said to be a normal subgroup of G if for every $x \in G$ and for every $h \in H$, $xhx^{-1} \in H$.

i.e H is a Normal subgroup of G if and only if $xHx^{-1} \subseteq H$ $\forall x \in G$. and $\forall h \in H$.

Theorem A subgroup H of a group G is normal if and only if $xHx^{-1} = H$ $\forall x \in G$.

proof → Let $xHx^{-1} = H$ $\forall x \in G$. Then $xHx^{-1} \subseteq H$ $\forall x \in G$

Therefore H is a Normal subgroup of G.

Converse Let H be a Normal subgroup of G.

Then $xHx^{-1} \subseteq H$ $\forall x \in G$. ——(1)

Also $x \in G \Rightarrow x^{-1} \in G$. Therefore we have

$x^{-1}H(x^{-1})^{-1} \subseteq H \; \forall \; x \in G$

$\Rightarrow x^{-1}Hx \subseteq H \; \forall \; x \in G$

$\Rightarrow x(x^{-1}Hx)x^{-1} \subseteq xHx^{-1} \; \forall \; x \in G.$

$\Rightarrow xH \subseteq xHx^{-1}$ for all $x \in G$. — (2)

from (1) and (2) we get

$xHx^{-1} = H$ for all $x \in G$.

Theorem 2. A subgroup H of a group G is a Normal subgroup of G if and only if each left coset of H in G is a right coset of H in G.

Proof : Let H be a Normal subgroup of G.

Then $xHx^{-1} = H \; \forall \; x \in G$

$\Rightarrow (xHx^{-1})x = Hx$ for all $x \in G$

$\Rightarrow xH = Hx$ for all $x \in G$

$\Rightarrow$ each left coset xH is the right coset Hx

Conversely suppose that each left coset of H in G is a right coset of H in G. Let x be any element of G. Then

$xH = Hy$ for some $y \in G$.

Since $e \in H$, therefore $xe = x \in xH$

$\therefore x \in Hy$ ($\because Hy = Hx$)

But $x \in Hy \Rightarrow Hx = Hy$

$\therefore Hx = xH$

Thus we have

$xH = Hx \quad \forall x \in G$

$\Rightarrow xHx^{-1} = Hxx^{-1} \quad \forall x \in G$

$\Rightarrow xHx^{-1} = H \quad \forall x \in G$

$\Rightarrow H$ is a Normal subgroup of G.

Thus H is a Normal subgroup of G

$\Leftrightarrow xH = Hx \quad \forall x \in G$.

Homeomorphism :

Let $(S, *)$ and $(S_2, \otimes)$ be two semigroup. Then the function f from S_1 to S_2 is homeomorphism provided

(a) f is one-one onto function and

(b) $f(a * b) = f(a) \otimes f(b)$

ILLUSTRATION → Let $A = \{0, 1\}$ be a set and $(S, \times)$ and $(S_2, +)$ be two semigroups, where operation $+$ is defined as

+	0	1
0	0	1
1	1	0

A function from S_1 to S_2 is defined as $f: S_1 \to S_2$ such that for all $a \in S_1$

$$f(a) = \begin{cases} 1 & \text{if } A \text{ has an odd Number of 1s} \\ 0 & \text{if } A \text{ has even Number of 1s} \end{cases}$$

This definition of $f(a)$ implies that for any elements $x, y \in S_1$

We have $f(x,y) = f(x) + f(y)$. Obviously f is onto because $f(0)=0$ and $f(1)=1$. Thus, f is a homeomorphism.

Example:

The mapping defined as

$f: I \to \{1, -1\}$ such that $f(n)=1$ when n is even and $f(n) = -1$ when n is odd, is a group homeomorphism because $f(m+n) = f(m) f(n)$ for all $m, n \in I$

Isomorphism → Let $(S_1, *)$ and $(S_2, \otimes)$ be two semigroup. A function f from S_1 to S_2 is an isomorphism if

(i) f is a bijection (one-one onto) function, and

(ii) $f(a * b) = f(a) \otimes f(b)$ for all $a, b \in S_1$

If such a function exists, then S_1 is isomorphic to S_2 and is written as $S_1 \simeq S_2$

Since f is one-one onto therefore, inverse function, f^{-1} exists from S_2 to S_1 and hence, also an isomorphism between $(S_2, \otimes)$ and $(S_1, *)$.

ILLUSTRATION.

Let $S_1 = \{a, b, c\}$ and $S_2 = \{1, \omega, \omega^2\}$ be two sets. Let $f: S_1 \to S_2$ be defined as $f(a) = 1$, $f(b) = \omega$ and $f(c) = \omega^2$

Then the following tables show that f is one-one onto. Thus f is homeomorphism as well as isomorphism between S_1 and S_2 with binary operation $*$ and $\otimes$, and hence $(S_1, *)$ and $(S_2, \otimes)$ are isomorphic semigroup

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

$\otimes$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

It may be noted that the table for S_2 is obtained by replacing elements in S_1 by their image

Example → Let A be the set of 2×2 Matrices. Show that semigroups, $A = \left[\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}, \times\right]$ and

$(R, +)$ are isomorphism.

Sol: We defined the function $f: R \to A$ by $f(a) = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$, for all $a \in R$

To prove f to be one-one, suppose $f(a_1) = f(a_2)$. Then

$$\begin{bmatrix} 1 & a_1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a_2 \\ 0 & 1 \end{bmatrix} \text{ or } a_1 = a_2$$

Hence f is a one-one function
Also suppose that $b \in R$ is any real number. Then

$$f(a) = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$$

So f is a onto function
For $a, b \in R$ we have

$$f(a)\,f(b) = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix}$$

$$= f(a+b)$$

Since both properties of isomorphism are satisfied therefore, A and R are isomorphic semigroups.

Algebraic structure with two binary operation

* RING

Definition → Suppose R is a non-empty set with two binary operation, called addition (+) and multiplication (·). Then the Mathematical structure $(R, +, \cdot)$ is called a ring if the following conditions are satisfied

1. $(R, +)$ is an abelian group

(i) Closure law → $a+b \in R$ for all $a, b \in R$

(ii) Associative law → $a+(b+c) = (a+b)+c$ for all $a, b, c \in R$

(iii) Additive Identity → There exist an element $0 \in R$ called the identity element such that

$0+a = a+0$ for all $a \in R$

The element $0 \in R$ is called the zero element of the ring

(iv) Additive Inverse → $a, b \in R$ for all $a, b \in R$.

Then b is called the inverse of

Date.
Page No.

a and is denoted by (-a)

(v) Addition is commutative
$a+b = b+a$ for all $a, b \in R$

2. closure and Associative law for multiplication.

(i) closure law :
$a \cdot b \in R$ for all $a, b \in R$.

(ii) Associative law
$a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in R$

3. Distributive law :

Multiplication is distributive with respect to addition.
i.e for all $a, b, c \in R$.
$a \cdot (b+c) = b \cdot c + c \cdot a$
and $(b+c) \cdot a = b \cdot a + c \cdot a$

Date: _____
Page No. _____

Properties of a Ring

If the algebraic structure $(R, +, \cdot)$ is a ring, then for all $a, b, c \in R$, the following properties are satisfied.

1. $a \cdot 0 = 0 \cdot a = 0$
2. $a \cdot (-b) = -(a \cdot b) = (-a) \cdot b$
3. $(-a)(-b) = a \cdot b$
4. $a \cdot (b - c) = a \cdot b - a \cdot c$
5. $(b - c) \cdot a = b \cdot a - c \cdot a$

Q1. Prove that the set $S = \{0, 1, 2, 3, 4\}$ is a ring with respect to the operation of addition and multiplication modulo 5.

Sol: Forming the composition tables for the two operations $+_5$ and $\times_5$ as

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

It is easy to prove from the first table that the structure $(S, +_5)$ is an abelian group.

from the second composition table we see that S is closed with respect to the operation $\times_5$.

Since S being a set of Numbers, we have

(i) $(a \times_5 b) \times_5 c = a \times_5 \{(b \times_5 c)\}$

$\forall$ a, b, c $\in$ c.

(ii) $a \times_5 \{(b +_5 c)\} = (a \times_5 b) +_5 (a \times_5 c)$

and $(b +_5 c) \times_5 a = (b \times_5 a) +_5 (c \times_5 a)$

$\forall$ a, b, c $\in$ S

Hence S is a ring with respect to the given operations.

Integral Domain]

A commutative ring with unity containing no zero divisors is called an integral domain. It is usually denoted by $(D, +, *)$.

In other words a ring is also integral domain, if it

(i) is commutative
(ii) has unit element
(iii) is without zero divisors.

ILLUSTRATIONS]

1. The set of integers I is an integral domain. It has been earlier proved that I is a commutative ring with unity. Also I does not have zero divisors. We know that if $a, b \in I$ such that $a \cdot b = 0$ then either a or b (or both) is zero

2. The ring R of Numbers: $a + \sqrt{2}b$ $a, b \in I$ is an integral domain R is commutative ring with

unity

$(a+\sqrt{2}b)(c+\sqrt{2}d)$

$= ac + \sqrt{2}bc + \sqrt{2}ad + 2bd = 0$

$= (ac+2bd) + (bc+ad)\sqrt{2} = 0$

only if $ac+2bd = 0$ and $(bc+ad)\sqrt{2} = 0$

implies that either

$a+\sqrt{2}b = 0$ or $c+\sqrt{2}b = 0$

Homeomorphism :

Let $(S, *)$ and $(S_2, \otimes)$ be two semigroup. Then the function f from S_1 to S_2 is homeomorphism provided

(a) f is one-one onto function and

(b) $f(a * b) = f(a) \otimes f(b)$

ILLUSTRATION → Let $A = \{0, 1\}$ be a set and $(S_1, \times)$ and $(S_2, +)$ be two semigroups, where operation $+$ is defined as

+	0	1
0	0	1
1	1	0

A function from S_1 to S_2 is defined as $f : S_1 \to S_2$ such that for all $a \in S_1$

$$f(a) = \begin{cases} 1 & \text{if } A \text{ has an odd Number of 1s} \\ 0 & \text{if } A \text{ has even Number of 1s} \end{cases}$$

This definition of $f(a)$ implies that for any elements $x, y \in S_1$

We have $f(x+y) = f(x) + f(y)$. Obviously f is onto because $f(0)=0$ and $f(1)=1$. Thus, f is a homeomorphism.

Example.

The mapping defined as

$f: I \to \{1, -1\}$ such that $f(n)=1$ when n is even and $f(n) = -1$ when n is odd, is a group homeomorphism because $f(m+n) = f(m) f(n)$ for all $m, n \in I$.

Isomorphism → Let $(S_1, *)$ and $(S_2, \otimes)$ be two semigroup. A function f from S_1 to S_2 is an isomorphism if

(i) f is a bijection (one-one onto) function, and

(ii) $f(a * b) = f(a) \otimes f(b)$ for all $a, b \in S_1$.

If such a function exists, then S_1 is isomorphic to S_2 and is written as $S_1 \simeq S_2$.

Since f is one-one onto therefore, inverse function, f^{-1} exists from S_2 to S_1 and hence, also an isomorphism between $(S_2, \otimes)$ and $(S_1, *)$.

ILLUSTRATION.

Let $S_1 = \{a, b, c\}$ and $S_2 = \{1, \omega, \omega^2\}$ be two sets. Let $f: S_1 \to S_2$ be defined as $f(a) = 1$, $f(b) = \omega$ and $f(c) = \omega^2$

Then the following tables show that f is one-one onto. Thus f is homeomorphism as well as isomorphism between S_1 and S_2 with binary operation $*$ and $\otimes$, and hence $(S_1, *)$ and $(S_2, \otimes)$ are isomorphic semigroup

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

$\otimes$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

It may be noted that the table for S_2 is obtained by replacing elements in S_1 by their images

Example → Let A be the set of 2×2 Matrices. Show that semigroups, $A = \left[\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}, \times\right]$ and

$(R, +)$ are isomorphism.

Soln We defined the function $f: R \to A$ by $f(a) = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$, for all $a \in R$

To prove f to be one-one, suppose $f(a_1) = f(a_2)$. Then

$$\begin{bmatrix} 1 & a_1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a_2 \\ 0 & 1 \end{bmatrix} \text{ or } a_1 = a_2$$

Hence f is a one-one function Also suppose that $b \in R$ is any Real Number. Then

$$f(a) = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$$

So f is a onto function For $a, b \in R$ we have

$$f(a)\,f(b) = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix}$$

$$= f(a+b)$$

Since both properties of isomorphism are satisfied therefore, A and R are isomorphic semigroups.

Algebraic structure with two binary operation

* RING

Definition → Suppose R is a non-empty set with two binary operation, called addition (+) and multiplication (·). Then the Mathematical structure $(R, +, \cdot)$ is called a ring if the following conditions are satisfied

1. $(R, +)$ is an abelian group

(i) Closure law → $a+b \in R$ for all $a, b \in R$

(ii) Associative law → $a+(b+c) = (a+b)+c$ for all $a, b, c \in R$

(iii) Additive Identity → There exist an element $0 \in R$ called the identity element such that

$0+a = a+0$ for all $a \in R$

The element $0 \in R$ is called the zero element of the ring

(iv) Additive Inverse → $a.b \in R$ for all $a, b \in R$.

Then b is called the inverse of

Date.
Page No.

a and it denoted by (-a)

(v) Addition is commutative
$a+b = b+a$ for all $a, b \in R$

2. closure and Associative law for multiplication.

(i) closure law :
$a \cdot b \in R$ for all $a, b \in R$.

(ii) Associative law
$a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in R$

3. Distributive law :

Multiplication is distributive with respect to addition.
i.e for all $a, b, c \in R$.
$a \cdot (b+c) = b \cdot c + c \cdot a$
and $(b+c) \cdot a = b \cdot a + c \cdot a$

Page No. _____

Properties of a Ring

If the algebraic structure $(R, +, \cdot)$ is a ring, then for all $a, b, c \in R$, the following properties are satisfied.

1. $a \cdot 0 = 0 \cdot a = 0$
2. $a \cdot (-b) = -(a \cdot b) = (-a) \cdot b$
3. $(-a)(-b) = a \cdot b$
4. $a \cdot (b - c) = a \cdot b - a \cdot c$
5. $(b - c) \cdot a = b \cdot a - c \cdot a$

Q1. Prove that the set $S = \{0, 1, 2, 3, 4\}$ is a ring with respect to the operation of addition and multiplication modulo 5.

Sol'n Forming the composition tables for the two operations $+_5$ and $\times_5$ as

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

It is easy to prove from the first table that the structure $(S, +_5)$ is an abelian group

from the second composition table we see that S is closed with respect to the operation $\times_5$

Since S being a set of Numbers, we have

(i) $(a \times_5 b) \times_5 c = a \times_5 \{(b \times_5 c)\}$

$\forall$ ~~all~~ $a, b, c \in S$.

(ii) $a \times_5 \{(b +_5 c)\} = (a \times_5 b) +_5 (a \times_5 c)$

and $(b +_5 c) \times_5 a = (b \times_5 a) +_5 (c \times_5 a)$

$\forall$ $a, b, c \in S$

Hence S is a ring with respect to the given operations

Integral Domain]

A commutative ring with unity containing no zero divisors is called an integral domain. It is usually denoted by $(D, +, *)$.

In other words a ring is also integral domain, if it

(i) is commutative
(ii) has unit element
(iii) is without zero divisors.

ILLUSTRATIONS]

1. The set of integers I is an ~~integers~~ integral domain. It has been earlier proved that I is a commutative ring with unity. Also I does not have zero divisors. We know that if $a, b \in I$ such that $a \cdot b = 0$ then either a or b (or both) is zero

2. The ring R of Numbers: $a + \sqrt{2}b$ $a, b \in I$ is an integral domain R is commutative ring with

unity

$(a+\sqrt{2}b)(c+\sqrt{2}d)$

$= ac + \sqrt{2}bc + \sqrt{2}ad + 2bd = 0$

$= (ac+2bd) + (bc+ad)\sqrt{2} = 0$

only if $ac+2bd = 0$ and $(bc+ad)\sqrt{2} = 0$

implies that either

$a+\sqrt{2}b = 0$ or $c+\sqrt{2}b = 0$

Date: _____
Page No. _____

Q Suppose M is a ring of all 2×2 matrices with their elements as integers, the addition and Multiplication of matrices being the two ring Compositions. Then M is a ring with zero divisors.

Soln The null Matrix $O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ is the zero element of this ring.

Now $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ are two non zero elements of this ring. i.e $A \neq 0$, $B \neq 0$ we have

$$AB = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0$$

Thus the product of two Non-zero elements of the ring is equal to the zero element of the ring. Therefore M is a ring with zero divisor.

Also it is intresting to Note that

$$BA = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Thus in a ring R it is possible that $ab = 0$ but $ba \neq 0$.

Field → A Ring R with at least two element is called a field if it,

(i) is commutative

(ii) has Unity

(iii) is such that each non zero element possesses multiplicative inv

Q. Show that the set of Number of the form $a+b\sqrt{2}$ with a and b as rational Number is a field.

Sol/ Let $R = \{a+b\sqrt{2} : a, b \in Q\}$

Let $a_1+b_1\sqrt{2} \in R$ and

$a_2+b_2\sqrt{2} \in R$ Then

$a_1, b_1, a_2, b_2 \in Q$.

We have

$(a_1+b_1\sqrt{2}) + (a_2+b_2\sqrt{2})$

$= (a_1+a_2) + (b_1+b_2)\sqrt{2}$

$\in R$ since $a_1+a_2, b_1+b_2 \in Q$

Thus R is closed with respect to addition and Multiplication, All the element of R are Rel Number and we know that addition and multiplication are both associative as well as

Date:
Page No.

Commutative compositions in the set of real Numbers.
further we have
$a+0\sqrt{2} \in R$ since $0 \in Q$
If $a+b\sqrt{2} \in R$ then
$(0+0\sqrt{2})+(a+b\sqrt{2})$
$= (0+a)+(0+b)\sqrt{2} = a+b\sqrt{2}$
$0+0\sqrt{2}$ is the additive identity
each element of R possesses additive inverse
Further in the set of real Number multiplication is distributive with respect to addition.
Again
$1+0\sqrt{2} \in R$ and we have
$(1+0\sqrt{2})(a+b\sqrt{2}) = a+b\sqrt{2}$
$= (a+b\sqrt{2})(1+0\sqrt{2})$
$\therefore 1+0\sqrt{2}$ is the multiplicative identity
Thus R is a commutative ring with unity. The zero element of the ring $0+0\sqrt{2}$ and the unit element is $1+0\sqrt{2}$.
Now R will be a field if each non zero element of R possesses multiplicative inverse.

Page No.

Let $a+b\sqrt{2}$ be any non-zero element of this ring i.e at least one of a and b is not zero

Then

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})}$$

$$= \frac{a-b\sqrt{2}}{a^2-2b^2}$$

$$= \left(\frac{a}{a^2-2b^2}\right) + \left(-\frac{b}{a^2-2b^2}\right)\sqrt{2}$$

$\frac{a}{a^2-2b^2}$ and $\left(-\left(\frac{b}{a^2-2b^2}\right)\right)\sqrt{2}$ is a non zero element of R and is the multiplicative inverse of $a+b\sqrt{2}$.

Hence the given system is a field.

Date. _____
Page No. _____

Boolean Algebra

Def → A Non empty Set B containing at least two distinct element 0 and 1, with two binary operation '+' (OR) and '.' (AND) as well as a unary operation '-' (NOT) is called a Boolean algebra denoted by $(B, +, -, 0, 1)$ if and only if following axioms are satisfied.

(i) **Commutative laws**

$$a + b = b + a$$

and $a \cdot b = b \cdot a \quad \forall\ a, b \in B.$

(ii) **Distributive laws →**

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

and $a + (b \cdot c) = (a + b) \cdot (a + c) \quad \forall a, b, c \in$

(iii) **Identity laws →**

$$a + 0 = 0 + a = a$$

and $a \cdot 1 = 1 \cdot a = a \quad \forall\ a \in B.$

(iv) **Complement law →**

$$a + \bar{a} = \bar{a} + a = 1$$

Date.
Page No.

The element $\bar{a}$ is said to be the complement of the element $a \in A$ with respect to the operation $(+)$ if

$$a \cdot \bar{a} = \bar{a} \cdot a = 0$$

then $\bar{a}$ is said to be Complement of the element $a \in A$ with respect to the operation $(\cdot)$.

Date.
Page No.

Definition 2 :-

Let $A = \{p, q, r \ldots\}$ be any Set of Statement and let $\vee$ (OR), $\wedge$ (AND) and $\sim$ (Negation) be binary operation defined on A. Then the Mathematical Structure $[A, \vee, \wedge, \sim]$ is called a Boolean algebra if and only if the following axioms are satisfied.

(i) Commutative laws

$p \vee q \Leftrightarrow q \vee p$
and $p \wedge q \Leftrightarrow q \wedge p \quad \forall\ p, q \in A.$

(ii) Distributive laws
$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$
and $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r).$
$\forall\ p, q, r \in A$

(iii) Identity laws $p \vee 0 = 0 \vee p = p$
and $p \wedge 1 = 1 \wedge p = p \quad \forall\ p \in A$

(iv) Complement laws

$p \vee \sim p = 1$
and $p \wedge \sim p = 0 \quad \forall\ p \in A$

8. (v) De- Morgan's law

(i) $\sim(p \wedge q) \Leftrightarrow p \vee \sim q$

(ii) $\sim(p \vee q) \Leftrightarrow \sim p \wedge \sim q$.

Example

Let $B = \{0, 1\}$ given set are finite then prepare a Composition table

+	0	1
0	0	1
1	1	0

*	0	1
0	0	0
1	0	1

'	
0	1
1	0

(1) Commutative law

We see from table + and * operation respectively $\forall a, b \in B$

Then $a+b = b+a$

also $a \times b = b \times a$

Date.
Page No.

Let $a=1, b=0$

$a+b = 1+0 = 1$

$b+a = 0+1 = 1$

$a \times b = 1 \times 0$

$= 0$

$b \times a = 0 \times 1 = 0$

(2) Identity law

from table 0 is the identity element with respect to addition and 1 is the identity from multiplication.

(3) Distributive law :

$a \times (b+1) = (a \times b) + (a \times c)$

Also $a + (b \times c) = (a+b) \times (a+c)$

$a=0, \quad b=1, \quad c=1$

$a \times (b+1) = 0 \times (1+1)$

$= 0 \times 1$

$= 0$

Again $(a \times b) + (a \times c)$

$= (0 \times 1) + (0 \times 1)$

$= 0 + 0 = 0$

(4) Complement law

$$a + \bar{a} = 1$$

$$0 + 1 = 1$$

$$0' = 1$$

$$1' = 0$$

All property satisfying the B is a boolean Algebra

Date.
Page No.

Boolean Ring :-

Definition :- A Ring $(R, +, \cdot)$ is said to be Boolean Ring if
$a^2 = a \quad \forall a \in R$
$a^2 = a$ (idempotent law)

Example $(Z_2, +_2, \times_2)$ $Z_2 = \{0, 1\}$

$0^2 = 0$
$1^2 = 1$

$\therefore$ Z_2 is a boolean ring

Result Every Boolean Ring is Commutative

Proof :- Let R be a Boolean Ring i.e
$a^2 = a \quad \forall a \in R$

To show that R is commutat
i.e. $ab = ba \quad \forall a, b \in R$.

Step 1 Consider $(a+a)^2 = a+a \quad \forall a$
(as $a+a \in R$) (by $\oplus$)

i.e $(a+a)(a+a) = a+a$

i.e $a^2+a^2+a^2+a^2 = a+a$

i.e $a+a+a+a$

$= a+a \quad \forall a \in R$ (by $\oplus$)

i.e $a+a = 0 \quad \forall a \in R$ (by cancellation law of addition)

Step 2) Consider $(a+b)^2 = a+b$

$\forall\ a, b \in R \Rightarrow a+b \in R$ (by ①)

i.e $(a+b)(a+b) = a+b$

i.e $a^2 + ab + ba + b^2 = a+b$

i.e ~~$a+b$~~ $a + ab + ba + b$

$= a+b \quad \forall\ a, b \in R$ (by ①)

i.e $ab + ba = 0 \quad \forall\ a, b \in R$

(by cancellation law of addition)

i.e $ab = -ba = b(-a)$

i.e $ab = ba \quad \forall\ a, b \in R$ (by ①)

Date.
Page No.

Congruence Relation :

Let m be a positive integer. Then an integer a is said to be congruent to another integer b modulo m provided m divides $a-b$. Symbolically, we have

$a \equiv b \pmod{m}$ or $a \equiv b \pmod m$

It is read as 'a is congruent to b modulo m. Then integer m is called the modulus and b is called a residue of a (mod m)

The Negation of $a \equiv b \pmod m$ is written as $a \not\equiv b \pmod m$ and in such a case integers a and b are said to be incongruent modulo m.

From the definition of congruence, it may be concluded that $a \equiv b \pmod m$ provided $a - b = km$ or ~~$a-b=$~~

$a = b + km$ for some integer k.

Illustrations

$89 \equiv 25 \pmod 4$, since $89 - 25 = 64$ is divisible by 4. Consequently 25 is the residue of 89 (mod 4) and 4 is the modulus of the congruence.

Date.
Page No.

Example find the least positive integers modulo 5 to which 19, 288 and -28 are congruent

Sol. $19 = 5 \times 3 + 4 \Rightarrow 19 \equiv 4 \pmod 5$

$288 = 5 \times 57 + 3 \Rightarrow 288 \equiv 3 \pmod 5$

$-28 = 5 \times (-6) + 2 \Rightarrow -28 \equiv 2 \pmod 5$

Quotient Group (structure)

Let G be group and N is a Normal subgroup
Then $\frac{G}{N}$ is called the quotient group where $\frac{G}{N}$ is the group of all left/right cosets of N

i.e $\frac{G}{N} = \{aN \ \forall \ a \in G\}$

$\frac{G}{N} = \{aN \ \forall \ a \in G\}$

Now we can show that $\frac{G}{N}$ is a group.

(1) closure properties

$aN * bN = (a*b)N \ \forall \ a, b \in G$

(2) Associative properties →

$(aN * bN) * cN = aN * (bN * cN)$
$= (a*b*c)N$

(3) Identity properties →

$aN * eN = aN$
$= (a*e)N$
$= aN.$

(4) Inverse properties :-

for aN. $\exists\ a^{-1} \in N$

i.e $aN * a^{-1}N = (a * a^{-1})N$

$eN = N$.