# ALGEBRA

**Unit 1.**

## Preliminaries

**Relation.**

Let A and B be non-empty sets. A subset $\rho$ of A x B is called a relation or binary relation from A to B. i.e. If an ordered pair $(a,b) \in \rho$, then we say that a is related to b and it is denoted by $a \rho b$.

**Examples.**

1. In **Z,** $a \rho b$ means $a \leq b$
2. In **Z,** $a \rho b$ means $a < b$
3. In **Z,** $a \rho b$ means a divides b
4. In **Z,** $a \rho b$ means ab is even
5. In **Z,** $a \rho b$ means ab is perfect square. etc….

**Equivalence Relation.**

A relation $\rho$ on a set A is said to be equivalence relation if

(i) Reflexive. $a\rho a$.

(ii) Symmetric. If $a\rho b$ then $b\rho a$.

(iii) Transitive. If $a\rho b$, $b\rho c$ then $a\rho c$.

Ex.

Let S = Z. $a\rho b$ means $a \equiv b \pmod{m}$.

To Prove that $\rho$ is an equivalence relation.

Proof.

$a \equiv b \pmod{m}$ means a-b is multiple of m.

(i). Reflexive.

Clearly $a - a = 0$ which is multiple of m.

$a \equiv a \pmod{m}$. $a\rho a$. Hence reflexive is true.

(ii). Symmetric.

Let $a \rho b$. To prove that $b \rho a$.

Since $a\rho b$, we have $a - b$ is multiple of m.

Therefore, $b-a$ is also multiple of m.

$b \equiv a \pmod{m}$ . Thus $b \rho a$.

(iii) Transitive.

Let a $\rho$b, b $\rho$ c then we have to prove that

a $\rho$ c.

a $\rho$ b implies a-b is multiple of m.

a – b = km …(1)where k is an integer.

b $\rho$ c implies b – c is multiple of m.

i.e b-c = $k_1$m…..(2), where $k_1$ is an integer.

Now, a -c = km +b -c = km + $k_1$m = (k+$k_1$) m

Therefore, a – c = $k_2$ m, where $k_2$ = k+$k_1$ is also an integer.

Hence a – c is multiple of m.

i.e a $\equiv$ c (mod m)

Hence a $\rho$ c. Thus transitive is true.

Thus " $\equiv$ " satisfies Reflexive, Symmetric and Transitive.

Hence $\equiv$ is an equivalence relation.

**PARTIAL ORDER RELATION.**

A relation is $\rho$ said to be a partial order relation if it satisfies the following three axioms.

(i). **Reflexive.** a $\rho$a

(ii). **Antisymmetric.**

If a$\rho$b, b$\rho$a then a = b

(iii). **Transitive.**

i.e if a$\rho$b and b$\rho$c then a$\rho$c.

Then $\rho$ is said to be partial order relation and the set ( S, $\rho$) is called **partial ordered set.**

**Example.**

**The set (N, $\leq$ ) is a partial ordered Set.**

**Proof.**

**(i). Reflexive.**

Clearly a $\leq$ a for all a $\in$N.

**(ii). Anti Symmetric.**

Let a$\leq$b, and b$\leq$ a. We have to prove that

a = b.

This is true only if a = b.

**(iii). Transitive.**

Let $a \leq b$ and $b \leq c$.

Then $a \leq b \leq c$.

Therefore $a \leq c$.

Hence transitive is true.

Thus "≤" satisfies reflexive, antisymmetric and transitive.

Hence, " ≤ " is partial order relation in N.

Thus (N, ≤) is a partial ordered set.

## GROUP.

**Definition.**

Let G be any set. Let * be binary operation defined in G. Then (G , *) is said to be a group if the following conditions are true.

(i). Closure Property.

For all $a, b \in G$, $a*b \in G$.

(ii) Associative Property.

$\forall a, b, c \in G$, $(a*b)*c = a*(b*c)$.

(iii) Existence of Identity.

There exists $e \in G$, such $a * e = e * a = a$.

(iv). Existence of Inverse.

For all $a \in G$, there exists $a^{-1} \in G$ , such that $a * a^{-1} = a^{-1} * a = e$.

**Abelian Group.**

A group ( G, *) is said to be abelian group if the commutative property is also true.

$a * b = b * a$ for all $a, b \in G$.

**Example.**

1. **Is ( N , +) is a group.**

(i) For all $a, b \in N$. $a + b$ is also in N.

Thus Closure property is true.

(ii). Associative.

Clearly for all $a, b, c \in N$ ,

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

Thus Associative is true.

(iii). Existence of Identity: $0 \notin N$.

Additive identity 0 not in N.

Thus (N, + ) is not a group.

2. **Example. ( N, .) is a group? Verify.**
   N = { 1, 2, 3,…..}
   ( N, .) is not a group.

3. **Example. Is (W +) , ( W, .) a group? Verify. W = { 0, 1, 2,….}**
4. **Example. ( Z, +) is a group or not.**
   Z = { ….-4,-3,-2,-1,0,1,2,3,4,……}
   Thus ( Z, +) is group. Also it is an abelian group.

5. **Example. Is ( Z , .) a group? Verify.**
   Closure , Associative, Identity is also true.
   Multiplicative inverse of Integers does not in Z
   Thus ( Z, .) is not group.

6. **Verify the following sets with binary operations are group or not.**
   (Q, +) (Q* ,.) , (R, +), (R*, .), (C ,+),
   ( C* , .)
   (Where Q* = Q – {0}, R* = R –{0}).

7. **Example.** Is ( Z, - ) a group?

   (i). Closure is true.
   (ii). Associative.
   3 – {5-(-6)}= 3 – 11 = 8
   (3-5) -(-6) = -2+6 = 4
   Associative is not true.
   ( Z , -) is not a group.

8. Verify G = { 1, -1, i, -i} is a group under usual multiplication?

   Proof. Cayley's table.

| . | 1 | -1 | i | -i |
|---|---|---|---|---|
| 1 | 1 | -1 | i | -i |
| -1 | -1 | 1 | -i | I |
| i | I | -i | -1 | 1 |
| -i | -i | I | 1 | -1 |

Hence (G , .) is a group.

9. **T**he set of all 2 x2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, where a, b, c, d are all real numbers is a group under matrix addition.

**Example 10.**

The set of all 2 x2 non-singular matrices is a group under multiplication.

**Example. 11**

Let G = $\{\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}, \begin{pmatrix}-1 & 0\\0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}\begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix}\}$.

Prove that G is a group under matrix multiplication, Construct the Cayley's table for this group.

**Proof.**

Let G = { I, A , B, C}, where I = $\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$, A = $\begin{pmatrix}-1 & 0\\0 & 1\end{pmatrix}$, B = $\begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}$, and C = $\begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix}$

Now, IA = AI = A , IB = BI = B , IC = CI = C and I I = I.

And, AB = $\begin{pmatrix}-1 & 0\\0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\0 & -1\end{pmatrix} = \begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix}$ = C.

Similarly BA = $\begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}\begin{pmatrix}-1 & 0\\0 & 1\end{pmatrix} = \begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix}$ = C

Now, AC = $\begin{pmatrix}-1 & 0\\0 & 1\end{pmatrix}\begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix}=\begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}$ = B, and CA = B

Now, BC = $\begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}\begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix} = \begin{pmatrix}-1 & 0\\0 & 1\end{pmatrix}$ = A and CB = A.

Also, AA = BB = CC = I = $\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$

Hence Cayley's table is

| . | I | A | B | C |
|---|---|---|---|---|
| **I** | **I** | **A** | **B** | **C** |
| **A** | **A** | **I** | **C** | **B** |
| **B** | **B** | **C** | **I** | **A** |
| **C** | **C** | **B** | **A** | **I** |

**From cayley's table, closure , associative is true.**

**Identity is I.**

**Inverse of I, A, B, C is itself.**

**Hence** G =$\{\begin{pmatrix}1 & 0\\1 & 1\end{pmatrix}, \begin{pmatrix}-1 & 0\\0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}\begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix}\}$ is a group under matrix multiplication.

**Example 12.**

**Let G = { z / z∈C , and | z | = 1}. Then Prove that G is a group under usual multiplication.**

**Proof.**

(i). Closure Property.

Let $z_1, z_2 \in$G.

Then $| z_1| = | z_2 | = 1$

Therefore $|z_1 z_2| = |z_1|\,|z_2| = 1.1 = 1$.

Hence $z_1 z_2 \in G$.

Thus closure property is true.

(ii). Associative Property.

Clearly, $(z_1.z_2).z_3 = z_1.(z_2.z_3)$

We know that usual multiplication of complex numbers is associative.

(iii). Existence of Identity.

Now $1 = 1 + i0 \in G$ which is the identity element.

(iv). Existence of Inverse.

Let $z \in G$. Then $|z| = 1$.

Then $\left|\frac{1}{z}\right| = \frac{1}{|z|} = 1$.

Thus $\frac{1}{z} \in G$ and is the inverse of z.

Hence G is a group under usual multiplication.

**Definition.** **<u>Addition modulo n</u>**

Let $Z_n = \{0, 1, \ldots\ldots..(n-1)\}$.

Let $a, b \in Z_n$.

Let $a + b = qn + r$, where $0 \le r \le n$.

Then addition modulo n is defined by $a \oplus b = r$.

**Definition.** **<u>Multiplication modulo n</u>**

Let $Z_n = \{0, 1, \ldots\ldots..(n-1)\}$.

Let $a, b \in Z_n$.

Let $a . b = q'n + s$, where $0 \le s \le n$.

Then addition modulo n is defined by $a \circ b = s$.

**Example 13. Show that ( $Z_{12}$ , $\oplus$)** is a group.

| **$\oplus_{12}$** | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **0** | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** |
| **1** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **0** |
| **2** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **0** | **1** |
| **3** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **0** | **1** | **2** |
| **4** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **0** | **1** | **2** | **3** |
| **5** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **0** | **1** | **2** | **3** | **4** |
| **6** | **6** | **7** | **8** | **9** | **10** | **11** | **0** | **1** | **2** | **3** | **4** | **5** |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **7** | **7** | **8** | **9** | **10** | **11** | **0** | **1** | **2** | **3** | **4** | **5** | **6** |
| **8** | **8** | **9** | **10** | **11** | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** |
| **9** | **9** | **10** | **11** | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** |
| **10** | **10** | **11** | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** |
| **11** | **11** | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** |

Thus **(** $\mathbf{Z_{12}}$ **,** $\oplus$) is a group.

**Example 14. Prove that (** $\mathbf{Z_n}$ **,** $\oplus$) is a group.

Proof.

(i). Clearly $\oplus$ is a binary operation in $Z_n$.

(ii). Let a , b, c $\in Z_n$.

Let $a+b = q_1 n + r_1$……..(1)

$b+c = q_2 n + r_2$…………(2)

$r_1 + c = q_3 n + r_3$…………..(3) where $0 \leq r_1 \leq n.$ , $0 \leq r_2 \leq n$, $0 \leq r_3 \leq n$.

Now ( a+b) +c $= (q_1+q_3)n + r_3$ ( From (1) and (2)).

$\therefore$ $a + q_2 n + r_2 = (q_1+q_3)n + r_3$ (From (2))

$\therefore$ $a + r_2 = q_4 n + r_3$ (where $q_4 = q_1+q_3 - q_2$).

$(a \oplus b) \oplus c = r_1 \oplus c = r_3$ (from (3))

$a \oplus (b \oplus c) = a \oplus r_2 = r_3$

Thus $\oplus$ is associative.

Clearly the identity element is 0.

The inverse of $a \in Z_n$ is $n - a$.

**Hence (** $\mathbf{Z_n}$**,** $\oplus$**) is a group.**

**This group is called group of integers modulo n.**

**Example 15.**

If n is prime, then $Z_n - \{0\}$ is a group under multiplication modulo n.

**<u>Permutation Groups.</u>**

**Definition.**

Let A be any finite set. Then permutation of A is a bijection from A to A.

**Definition.**

Let A be a finite set consists of n elements. The set of all permutations of A is a group under the composition of functions. This group is called **Symmetric group** of degree n and is denoted by $\mathbf{S_n}$.

**Example.**

Let A = {1,2,3}. Then $S_3 = \{ e, p_1, p_2, p_3, p_4, p_5\}$

Where

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \ p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

**Cayley's table.**

| ∘ | e | $p_1$ | $p_2$ | $p_3$ | $p_4$ | $p_5$ |
|---|---|---|---|---|---|---|
| E | e | $p_1$ | $p_2$ | $p_3$ | $p_4$ | $p_5$ |
| $p_1$ | $p_1$ | $p_2$ | e | $p_4$ | $p_5$ | $p_3$ |
| $p_2$ | $p_2$ | e | $p_1$ | $p_5$ | $p_3$ | $p_4$ |
| $p_3$ | $p_3$ | $p_5$ | $p_4$ | e | $p_2$ | $p_1$ |
| $p_4$ | $p_4$ | $p_3$ | $p_5$ | $p_1$ | e | $p_2$ |
| $p_5$ | $p_5$ | $p_4$ | $p_3$ | $p_2$ | $p_1$ | e |

Then $S_3$ is a group under composition containing 3! elements.

**Order of a Group.**

If G is a finite group, then the number of elements in G is called order of G and it is denoted by o(G) or | G |.

**<u>Elementary Properties of Group.</u>**

- The identity element of group G is unique.
- For any a $\in$G, the inverse of a is unique.
- In a group the left and right cancellation laws hold.
  (i.e). ab = ac implies a = c and ba = ca implies b = c.
- Let G be a group and a, b $\in$ G. Then the equations ax = b and ya = b have unique solutions for x and y in G.
- In a Group G, for any a , b $\in$G, $(ab)^{-1} = b^{-1} a^{-1}$ and $(a^{-1})^{-1} = a$.