Unit—IV Algebraic Structure

Abstract Algebra: Abstract algebra is the study of algebraic structures. Algebraic structures include group, ring, field, module, vector space, lattices and algebras. The term abstract algebra was coined in the 20th century to distinguish this area of study from the other parts of algebra.

Other part of mathematics, concrete problems and examples have played important role in the development of abstract algebra.

Group theory has extensive applications in mathematics, science, and engineering. Many algebraic structures such as fields and vector spaces may be defined concisely in terms of groups, and group theory provides an important tool for studying symmetry, since the symmetries of any object form a group. Groups are thus essential abstractions in branches of physics involving symmetry principles, such as relativity, quantum mechanics, and particle physics. Furthermore, their ability to represent geometric transformations finds applications in chemistry, computer graphics, material sciences, cryptography and other fields.

Binary Operation: Let A and B be two sets. A function from $A \times A$ to B is called a binary operation on A. In simple words binary operation is a process that combines two elements of a set to obtain an element of a set. Binary operations are mostly denoted by $*, \#, +, \times, \cdot$ $, o, \cup, \cap, \odot, \otimes, \oplus$ etc.... If $*$ is a binary operation on a set A and $a, b \in A$, then $*\ (a, b)$ is generally written as $a * b$.

Example: Addition, subtraction, multiplication and division are binary operations on the set of integers.

Closure Property: A binary operation $*$ on a set A is called closed if $a * b \in A$ for all $a, b \in A$.

Example: Addition '$+$'on set of natural numbers $\mathbb{N}$ is a closed binary operation, since sum of two natural number is always a natural number. But subtraction '$-$' is not a closed binary operation on $\mathbb{N}$. Since, $1, 2 \ \in N$ but $1 - 2 \ \notin \ \mathbb{N}$.

Example: Set of irrational number under multiplication is not closed. $i.e.$ Multiplication is not closed on $\mathbb{R} - \mathbb{Q}$. Since $\sqrt{3} \times \sqrt{3} \ = \ 3 \notin \mathbb{R} - \mathbb{Q}$.

Algebraic Structure: A nonempty set S with a closed binary operation $*$ is called an algebraic system or algebraic structure and it is denoted by $(S,*)$.

Semigroup: A non-empty set S together with a binary operation $*$ is said to be a semigroup, if it satisfies the following properties:

(i) Closure: $a * b \in \ S, \ \forall \ a, b \in S$.

(ii) Associativity: $a * (b * c) = \ (a * b) * c, \forall \ a, b, c \in \ S$.

Examples

(i) Set of natural number under usual addition is a semigroup.

(ii) Set of even integers under addition is a semigroup.

(iii) The set of integers under subtraction is not a semigroup. Subtraction is not associative. If we take, $1, 2, 3 \in \mathbb{Z}$, then $1 - (2 - 3) \neq (1 - 2) - 3$.

(iv) A rectangular array of the form $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is said to be a 2× 2 matrix. The set of all 2×2 matrice with real enteries form a semigroup under component wise addition. That is

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{bmatrix}.$$

Cleary, it holds closure and associative properties.

Monoid: A non-empty set M together with a binary operation $*$ is said to be a monoid, if satisfies the following conditions:

(i) Closure: $a * b \in M; \forall\, a, b \in M$.

(ii) Associativity: $a * (b * c) = (a * b) * c;\ \forall\, a, b, c \in M$.

(iii) Identity: There exist an element $e \in M$ such that $a * e = e * a = a,\ \forall\, a \in M$.

Examples

(i) Set of integers $\mathbb{Z}$ under usual multiplication $\times$ form a monoid. As we know that multiplication of two integers is an integer, multiplication is closed on $\mathbb{Z}$. Since for any three integers k, l, m we have $(k \times l) \times m = k \times (l \times m)$, multiplication is associative on $\mathbb{Z}$. The integer 1 is the identity element as $k \times 1 = 1 \times k = k$. Hence $\mathbb{Z}$ is a monoid under usual multiplication.

(ii) $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{Q}, \times), (\mathbb{R}, +)$ and $(\mathbb{R}, \times)$ are monoids.

(iii) The set of complex number $\mathbb{C}$ is a monoid under addition $+$, where addition is defined as $(a + bi) + (c + di) = (a + c) + (b + d)i$.

(iv) Set of natural number under addition is not a monoid.

(v) Set of even integers under multiplication is not a monoid.

(vi) The set of all 2×2 matrice with real enteries form a monoid under usual matrix multiplication

Group: A non-empty set G, together with a binary operation $*$ is said to be form a group, if it satisfies the following properties:

(i) Closure: $a * b \epsilon G, \forall a, b \epsilon G$.

(ii) Associativity: $a * (b * c) = (a * b) * c, \forall a, b, c \epsilon G$.

(iii) Identity: There exists an element $e \epsilon G$ such that $a * e = e * a = a, \forall a \epsilon G$.

(iv) Existence of Inverse: $\forall a \epsilon G, \exists b \epsilon G$ (depending on a) such that $a * b = b * a = e$. The element b is called inverse of a.

Note: In a group $(G,*)$ identity element is unique and generally denoted by e. Inverse of an element a is unique and is denoted by a^{-1}. The element $a * a$ is denoted by a^2 and $a^n * a = a^{n+1}$ for any integer n. Also $a^0 = e$. We can write $a * b$ as ab, when the operation is well understood. **Order of a group G** is number of elements in G and it is denoted by $o(G)$ or $|G|$. **Order of an element a** is the least positive integer n such that $a^n = e$, where e is the identity element and is denoted by $o(a)$.

Examples

(i) $(\mathbb{Z}, +)$ is a group under usual addition. In verse of an integer m is $-m$.

(ii) $(\mathbb{Z}, \times)$ is not a group. Product of two integers is always an integer. Therefore, closure property hold. Since, $(a.b).c = a.(b.c) \; \forall \; a, b, c \in \mathbb{Z}$. So, associative hold. 1 is the identity element of $\mathbb{Z}$. Now, $2 \epsilon \mathbb{Z}$ but 2 has no inverse in $\mathbb{Z}$. There does not exist $a \epsilon \mathbb{Z}$ such that $a \times 2 = 2 \times a = 1$. Therefore, inverse property does not hold. Thus, set of integers under multiplication is not a group.

(iii) $(\mathbb{C}, +)$ is a group. But $(\mathbb{C}, \times)$ is not a group where × is the multiplication defined by $(a + ib).(c + id) = (ac - bd) + i(ad + bc)$.

(iv) Let G be the set $\{1, -1\}$. It is a group under usual multiplication.

$\times$	$\mathbf{1}$	$\mathbf{-1}$
$\mathbf{1}$	1	-1
$\mathbf{-1}$	-1	1

(v) The set of nonzero real numbers is a group under ordinary multiplication. The identity element is 1. The inverse of a is $\frac{1}{a}$.

(vi) $\mathbb{C}^* = \mathbb{C} = \{0\}$ form a group under usual multiplication. $1 = 1 + 0i$ is the identity element and $\frac{a-i}{a^2+b^2}$ is the inverse of $a + ib$.

(vii) The set of all 2×2 matrice with real enteries form a group under component wise addition. That is

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{bmatrix}.$$

The identity element is $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$.

(viii) The set $\mathbb{Z}_n = \{0, 1, 2, 3, \dots, n-1\}$ for $n \geq 1$ is a group under addition modulo n. The identity element is 0 and for any $j > 0 \in \mathbb{Z}_n$, the inverse of j is $n - j$. For the set $\mathbb{Z}_4 = \{0, 1, 2, 3\}$, we can form a table of operations as bellow:

mod 4	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

(ix) The set $\{1, 2, 3, \dots, n-1\}$ is a group under multiplication modulo n if and only if n is prime. That is $\mathbb{Z}_p - \{0\}$ is a group under multiplication modulo p if and only if p is a prime. $\mathbb{Z}_7$ is a group under multiplication modulo 7. This can verify by the table:

mod 7	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2

6	6	5	4	3	2	1

From the above table it is observed that 1 is the identity element and $2^{-1} = 4, 3^{-1} = 3, 5^{-1} = 5$.

(x) Let $U(n)$ the set of all positive integer less than n and relatively prime to n. That is $U(n) = \{m: 1 \leq m < n, \text{and } gcd\ (m, n) = 1\}$. Then $U(n)$ is a group under multiplication modulo n. For $n = 10$, $U(10) = \{1, 3, 7, 9\}$ is a group under multiplication modulo 10. The Cayley table for $U(10)$ is

mod 10	**1**	**3**	**7**	**9**
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

(xi) $G = \{1, -1, i, -i\}$ is a group under multiplication. This can be verified by the bellow table:

×	$\boldsymbol{1}$	$\boldsymbol{-1}$	$\boldsymbol{i}$	$\boldsymbol{-i}$
$\boldsymbol{1}$	1	-1	i	$-i$
$\boldsymbol{-1}$	-1	1	$-i$	i
$\boldsymbol{i}$	i	$-i$	-1	1
$\boldsymbol{-i}$	$-i$	i	1	1

From the table it is observed that the identity element is 1 and inverse of -1 is -1, inverse of i is $-i$.

(xii) The set $G = \{2, 4, 6, 8\}$ is a group under multiplication modulo 10. This can be shown in bellow table:

mod 10	2	4	6	8
2	4	8	2	6
4	8	6	4	2
6	2	4	6	8
8	6	2	8	4

(xiii) The set $G = \{1, 2, 3\}$ under multiplication modulo 4 is not a group as (2×2) mod $4 = 0 \notin G$.

Example: Check whether the following operation $*$ on real number form a group or not.

$$a * b = a + b - ab, \forall a, b \in \mathbb{R}.$$

Solution: (i) Closure:

$$a * b = a + b - ab \in \mathbb{R}, \qquad \forall a, b \in \mathbb{R}$$

(ii) Associative: We have to prove, $a * (b * c) = (a * b) * c$

$$a * (b * c) = a * (b + c - bc) = a + (b + c - bc) - a(b + c - bc)$$

$$a * (b * c) = a + b + c - bc - ab - ac + abc$$

$$a * (b * c) = a + b + c - ab - bc - ac + abc$$

Now,

$$(a * b) * c = (a + b - ab) * c = a + b - ab + c - (a + b - ab)c$$

$$(a * b) * c = a + b + c - ab - ac - bc + abc$$

$$(a * b) * c = a + b + c - ab - bc - ac + abc$$

Clearly, $a * (b * c) = (a * b) * c, \ \forall a, b, c \in \mathbb{R}$. Hence, associative property hold.

(iii) Identity: 0 is the identity element as

$$a * 0 = 0 * a = a + 0 - a.0 = a, \forall a \in \mathbb{R}.$$

(iv) Inverse: Let $a \in \mathbb{R}$, and $b \in \mathbb{R}$ such that

$$a * b = b * a = 0.$$

$$\Rightarrow a + b - ab = b + a - ba = 0$$

$$\Rightarrow a + b - ab = a + b - ab = a + b(1 - a) = 0$$

$$\Rightarrow b = \frac{-a}{1-a}, \text{ provided } a \neq 1.$$

Thus, inverse of 1 does not exist and hence $\mathbb{R}$ is not a group under the given binary operation. It is a monoid.

Some properties of Groups: In a group $(G,*)$

(i) Identity element is unique.

(ii) Inverse of an element is unique.

(iii) $(a^{-1})^{-1} = a, \forall a \in G.$

(iv) $(a * b)^{-1} = b^{-1} * a^{-1}$, $\forall a, b \in G.$

(v) $a * b = a * c$ implies $b = c$, and $b * a = c * a$ implies $b = c \; \forall a, b, c \in G.$

Proof: (i) Suppose e and e' be two identity elements of the group G. As, e is an identity and $e' \in G$,

$$e * e' = e' * e = e' \qquad (1)$$

Also, as e' is an identity and $e \in G$,

$$e' * e = e * e' = e \qquad (2)$$

Then from (1) and (2), we have $e = e'$.

(ii) Let $a \in G$ be any element and let a' and a'' be two inverses of a, then

$$a * a' = a' * a = e.$$

$$a * a'' = a'' * a = e.$$

Now,

$$a' = a' * e = a' * (a * a'') = (a' * a) * a'' = e * a'' = a''.$$

Hence, inverse of a is unique.

(iii) Since $a^{-1}$is inverse of a, $a * a^{-1} = a^{-1} * a = e$. Thus, a is inverse of a^{-1}. That is $(a^{-1})^{-1} = a$.

(iv) We have to prove $a * b$ has inverse $b^{-1} * a^{-1}$. That is

$$(a * b) * (b^{-1} * a^{-1}) = (b^{-1} * a^{-1}) * (a * b) = e.$$

Now,

$$(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = a * a^{-1} = e.$$

Similarly,

$$(b^{-1} * a^{-1}) * (a * b) = b^{-1} * (a^{-1} * a) * b = b^{-1} * e * b = b^{-1} * b = e.$$

Thus, $(a * b)^{-1} = b^{-1} * a^{-1}$, $\forall\, a, b \in G$.

(v) Let $a * b = a * c$. Then

$$b = e * b = (a^{-1} * a) * b = a^{-1} * (a * b) = a^{-1} * (a * c) = (a^{-1} * a) * c = e * c = c.$$

Thus, $a * b = a * c \Rightarrow b = c$.

Similarly, $b * a = c * a$ implies $a = c$.

Abelian Group: A group G is said to be an abelian group if $a * b = b * a$, $\forall\, a, b \in G$. An abelian group is also called a commutative group.

Examples:

(i) The set $(\mathbb{Z}, +)$ is an abelian group. Since, $a + b = b + a$, $\forall\, a, b \in \mathbb{Z}$.

(ii) Set of all 2×2 matrices over integers under addition form an abelian group.

(iii) Set of all 2×2 real matrices with non-zero determinant under matrix multiplication is a non-abelian group.

(iv) Let $G = \{0, 1, 2, 3, 4\}$ and define a binary operation $*$ on G by $a * b = (a + b) \text{mod } 5$. That is $a * b = c$, where c is least nonnegative integer obtained as remainder when $a + b$ divided by 5. Then G is an abelian group under the binary operation $*$.

(v) The set $G = \{1, -1, i, -i\}$ is an abelian group under multiplication.

(vi) The set of all permutations on a set of n elements is a non-abelian group under composition of functions.

Example: Let $G = \mathbb{R} - \{0\}$ and $a * b = \frac{ab}{2}$, $\forall$ a, b $\in G$. Show that $(G,*)$ is an abelian group.

Solution: (i) Closure: $a * b = \frac{ab}{2} \in G, \ \forall\, a, b \in G.$

(ii) Associative: $(a * b) * c = \frac{ab}{2} * c = \frac{abc}{4}.$

$$a * (b * c) = a * \left(\frac{bc}{2}\right) = \frac{abc}{4}.$$

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

(iii) Identity: $a * 2 = \frac{a.2}{2} = a, \ \ \forall\, a \in G.$

$$2 * a = \frac{2.a}{2} = a, \ \ \forall\, a \in G.$$

Hence 2 is the identity element of G.

(iv) Inverse: Let $a \in G$, and $b \in G$ such that

$$a * b = b * a = 2. \qquad \Rightarrow \frac{ab}{2} = \frac{ba}{2} = 2. \qquad \Rightarrow b = \frac{4}{a}.$$

Hence inverse of a exists and is $\frac{4}{a}$.

So, G is a group.

(v) $a * b = \frac{ab}{2}, \ \ b * a = \frac{ba}{2}$. $(\because ab = ba, \forall\, a, b \in \mathbb{R})$

$$\Rightarrow \quad a * b = b * a, \ \forall \ a, b \in G.$$

Thus, G is an abelian group.

Example: Show that in a group $(G,*)$, if $a^2 = e$. $\forall a \in G$, where e is the identity element, then G is a commutative group.

Solution: $a * b = e * a * b = (b * a)^2 * a * b = b * a * b * a * a * b$

$$= b * a * b * a^2 * b = b * a * b * e * b = b * a * b * b$$

$$= b * a * b^2 = b * a * e = b * a.$$

$\Rightarrow a * b = b * a, \ \forall a, b \in G,$ $\quad \Rightarrow$ G is an abelian group.

Alternative: Let $x \in G$, then

$$x^2 = e \Rightarrow x * x = e \Rightarrow x * x * x^{-1} = e * x^{-1} \Rightarrow x * e = x^{-1} \Rightarrow x = x^{-1}.$$

Thus, $\forall x \ \in G, x = x^{-1}$. Now for $a, b \in G$, we have,

$$a * b = (a * b)^{-1} = b^{-1} * a^{-1} = b * a.$$

Therefore, $(G,*)$ is an abelian group.

Cyclic Group: A group G is said to be cyclic if $\exists a \in G$ such that every element of G can be expressed as a power of a, i.e. $b = a^k$ for $b \in G$ and $k \in \mathbb{N}$. Then a is called a generator of group G and we write $G =< a >$. In other words, G is said to be a cyclic group if there exist an element $a \in G$ such that $G = \{a^n : n \in \mathbb{N}\}$.

Example: $G = \{1, -1, i, -i\}$ is a cyclic group under multiplication and i is a generator, as $i^1 = i, i^2 = -1, i^3 = -i, i^4 = 1$. Here, $-i$ is also a generator of G. Thus, i and $-i$ are generators of G.

Example: $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ is a group under addition modulo 5. One can verify that it is a cyclic group.

Example: Order of a cyclic group is equal to the order of its generator.