Abstract Algebra

Abstract algebra is a branch of mathematics that deals with algebraic structures such as groups, rings, fields, modules, vector spaces, and algebraic structures it is called abstract algebra.

- “Abstract" because of it deals with algebraic structures in a more general abstract way.

Why Abstract Algebra??

Abstract algebra is a fundamental branch of mathematics with broad applications across various fields.

1. **Cryptography and Coding Theory:**
2. **Problem Solving and Critical Thinking:**
3. **Algebraic Geometry:**
4. **Generalization of Algebraic Structures:**
5. **Computer Science:**

Finite Field

Definition:- A finite field is a set, equipped with two binary operations (addition and multiplication), where the set of non-zero elements forms a group under multiplication. Additionally, and both addition and multiplication operations satisfy closure, associativity, commutative, identity elements, and inverses.

Example: Finite Field F7:-

In the finite field F7, the elements are the residue classes modulo 7. The set of elements is {0, 1, 2, 3, 4, 5, 6}.

- **Addition (mod 7):**
  $2+6 \equiv 1 \pmod 7$
  $3+5 \equiv 1 \pmod 7$
  … And so on
- **Multiplication (mod 7):**
  $3 \times 5 \equiv 1 \pmod 7$
  $2 \times 4 \equiv 1 \pmod 7$
  … and so on.

Under addition and multiplication ((both performed modulo 7), this set forms a finite field. It satisfies all the properties of a field, including closure, associativity, commutatively, identity elements, and inverses

Group

Group:-A non-empty set A is said to be a group with respect to a binary operation *,if A satisfy clouser,associativity,identity, and inverse property with respect to *.

Closure property:-consider a non-empty set A and a binary operation * on A. A is said to be closed with respect to *,if $\forall a,b \in A$, then $a*b \in A$.

Algebraic structure:- consider a non-empty set A is said to be an algebraic structure with respect to a binary operation *,if $\forall a,b \in A$, then $a*b \in A$

Associativity property:- consider a non-empty set A and a binary operation * on A. A is said to be associative with respect to*,if ∀a,b,c ∈A, then (a*b)*c=a*(b*c).

Semi Group:-A non-empty set A is said to be a semi group with respect to a binary operation *,if A satisfy closure, associativity, property , with respect to *.

Identity property:-consider a non-empty set A and a binary operation * on A. A is said to be satisfy identity property with respect to *,if ∀a ∈A, then must be unique e ∈ A, such that

a*e=e*a=a

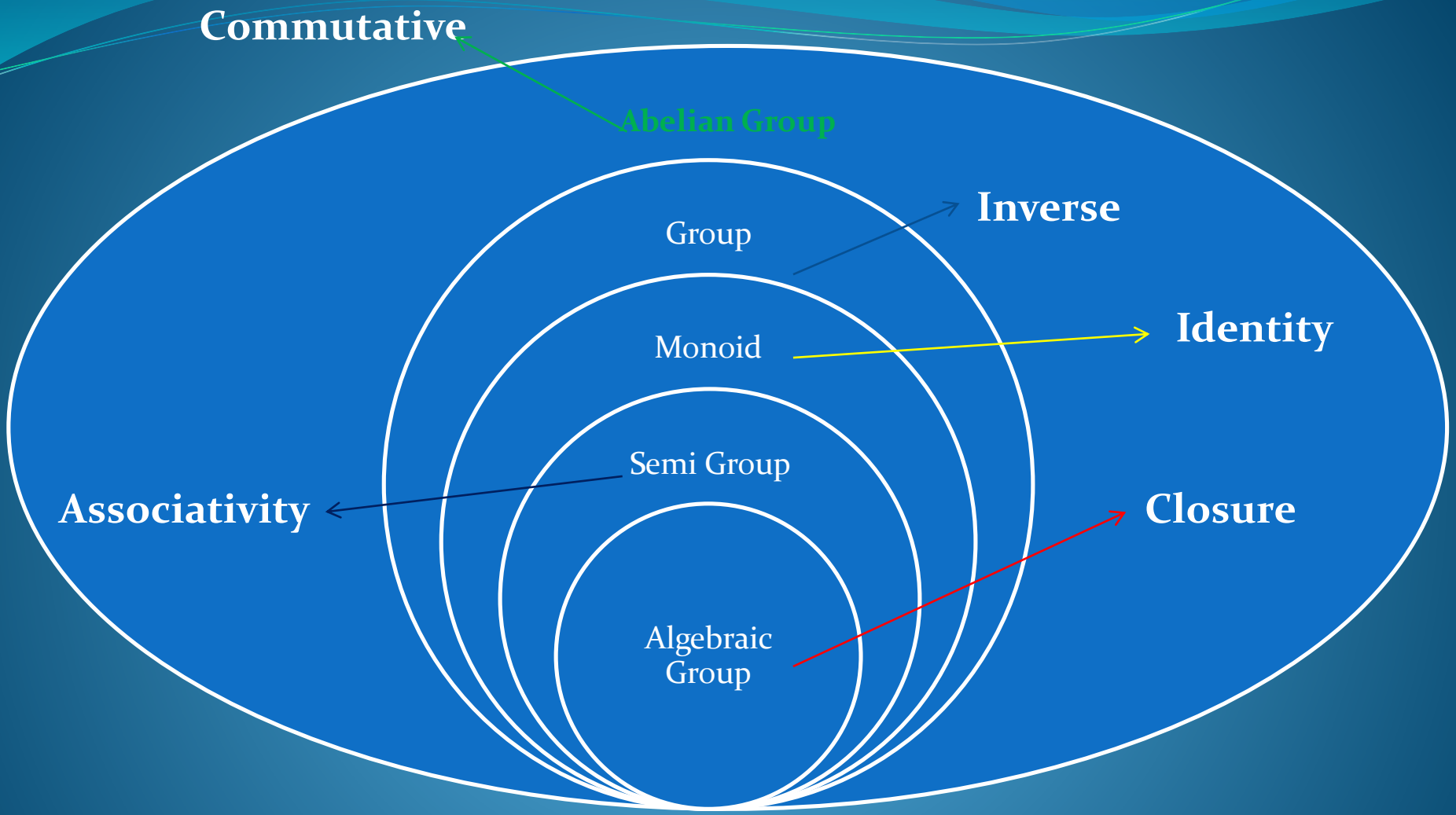
- There is exactly one identity element in the set and will be same for all element in the set

Monoid :-A non-empty set A is said to be a Monoid with respect to a binary operation *,if A satisfy closure, associativity, and identity property , with respect to *.

Inverse property:-consider a non-empty set A and a binary operation * on A. A is said to be satisfy inverse property with respect to *,if ∀a ∈A, there must be unique element a-1 ∈ A, such that

a* a-1 = a-1 *a=e

1. Every element has a exactly one unique inverse which is also present in the same set .
2. If a is the inverse of b then b will be inverse one a.
3. No two element s can have the same inverse.
4. Identity element is its own inverse.


Commutative
Abelian Group
Inverse
Group
Identity
Monoid
Semi Group
Associativity
Closure
Algebraic
Group

Example of Group

Real number R with + (addition):

G1: closure $x,y \varepsilon R \Rightarrow x+y \varepsilon R$

G2: Associativity $(x+y)+z = x + (y+z)$

G3: Identity element 0: $x + 0 = 0+x = x$

G4: Inverse of x is (-x): $x + (-x) = (-x) + x = 0$

G5: $x + y = y + x$

Another Example :-

Nonzero real numbers $R \setminus \{0\}$ with multiplication.

1. (G1) closure $x \neq 0$ and $y \neq 0 \Rightarrow xy \neq 0$
2. (G2) associative $(xy)z = x(yz)$
3. (G3) the identity element is 1 as $x1 = 1x = x$
4. (G4) the inverse of x is x^{-1} as $xx^{-1} = x^{-1}x = 1$
5. (G5) $xy = yx$ (commutative)

Theorem : The set Z*n which consists of all integers i=0,1, . . . ,n–1 for which gcd(i,n) = 1 forms an Abelian group under multiplication modulo n. The identity element is e = 1.

Example: If we choose n = 9, Z*9 consists of the elements {1,2,4,5,7,8}.
Multiplication table for Z*9
:

*mod9	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

Prove that it is a group

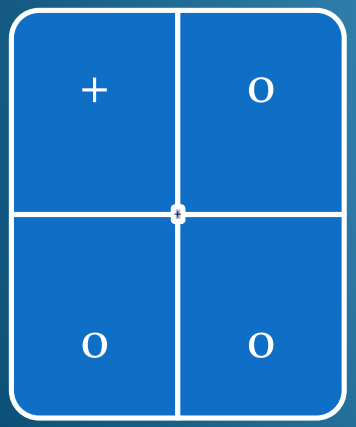
Note: Inverse a–1 of each element a ∈ Z ∗
n can be computed by using the extended Euclidean algorithm.

Finite Group

Finite Group:- A group with finite number of elements is called finite group.

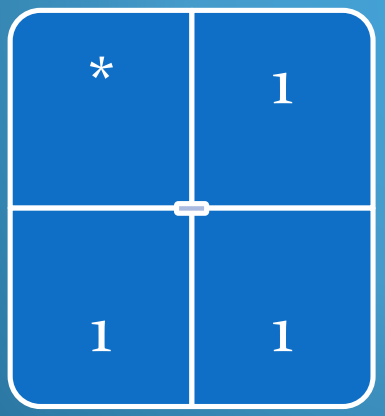
Example of Finite Group:-

{0}, +



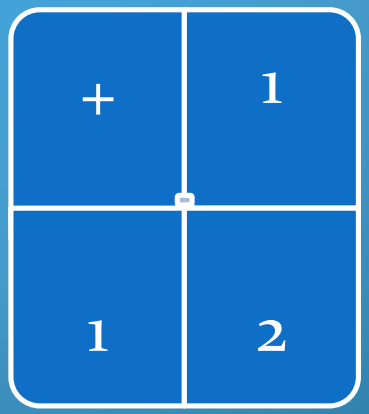
F.G

{1},*



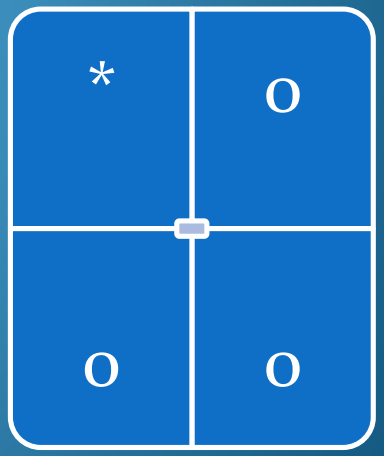
F.G

{1},+



N.F.G

{0},*



N.F.G

Another Example of F.G:-

{0,1}+ {0,1},* {−1,0,1}, + {−1,0,1},*

+	0	1
0	0	1
1	1	2

NFG

*	0	1
0	0	0
1	0	1

NFG

+	-1	0	1
-1	-2	-1	0
0	-1	0	1
1	0	1	2

NFG

*	-1	0	1
-1	1	0	-1
0	0	0	0
1	-1	0	1

NFG

$\{1, w, w2\}$,*

*	1	w	w2
1	1	w	w2
w	w	w2	1
w2	w2	1	w

$\{-1, 1, i, -i\}$,*

*	-1	1	i	-i
-1	1	-1	-i	i
1	-1	1	i	-i
i	-i	i	-1	1
-i	i	-i	1	-i

???

1. **Conclusion:- it is very difficult to design finite group as with number of greater than 2 closure property fails with simple addition and simple multiplication.**

2. **So we will try to develop new modified addition and multiplication operators with which closure and other properties can be satisfied**

Abelian Group:-A non-empty set A is said to be a an Abelian group with respect to a binary operation *,if A satisfy closure, associativity, identity inverse, and commutative property , with respect to *.

1. a*b = b*a
2. P*q=q*p

- **Note:- Matrices are not followed the Abelian group.**
- **Because of a*b≠ $b * a$.**

Order of an Element

The order ord(a) of an element a of a group $(G,\circ)$ is the smallest positive integer k such that

a

$k = a \circ a \circ \ldots \circ a = 1$

k times

where 1 is the identity element of G.

- If no such k exists, a is said to have infinite order, all elements of finite groups have finite order

Example :-

- We try to determine the order of a = 3 in the group Z^*_{11}

$a_1 = 3$

$a_2 = a \cdot a = 3 \cdot 3 = 9$

$a_3 = a_2 \cdot a = 9 \cdot 3 = 27 \equiv 5 \bmod 11$

$a_4 = a_3 \cdot a = 5 \cdot 3 = 15 \equiv 4 \bmod 11$

$a_5 = a_4 \cdot a = 4 \cdot 3 = 12 \equiv 1 \bmod 11$

From the last line it follows that $\mathrm{ord}(3) = 5$.

Generator of the Group

An element is called a generator if its order is
= number of elements in the group =|G|

- A group is cyclic if it contains a generator
- Cyclic Group: all the elements in the group can be obtained by repeatedly applying the group operation to a particular group element
- A cyclic group can have more than one generator

Generator Example

(z5, +) is a cyclic group :-

Since 3 ≡ 3 mod 5
3+3 ≡ 1 mod 5
3+3+3 ≡ 9 ≡ 4 mod 5
3+3+3+3 ≡ 12 ≡ 2 mod 5
3+3+3+3+3 ≡ 15 ≡ 0 mod 5
Ord(3) = |G| = 5 => Its a Cyclic Group
So all the group elements {0,1,2,3,4} in Z5 can be generated by 3
3 is also generator for the group Z5.

Another Example

$(z_5, +)$ is a cyclic group :-

Since $2 \equiv 2 \bmod 5$
$2+2 \equiv 4 \bmod 5$
$2+2+2 \equiv 6 \equiv 1 \bmod 5$
$2+2+2+2 \equiv 8 \equiv 3 \bmod 5$
$2+2+2+2+2 \equiv 10 \equiv 0 \bmod 5$
So all the group elements $\{0,1,2,3,4\}$ in Z_5

can also be generated by 2.
2 is a generator for the group Z_5

Cyclic Group

Cyclic Group:-A group (A,*) is said to be a cyclic group if it contains at least one generator.

1. **In a cyclic group if an element is a generator than its inverse will also be a generator.**
2. **The order of a cyclic group is always the order of the generating element of G.**

Generator

According to Langrage's Theorem:- let A be a cyclic group of order n, number of Generator in A is denoted by
$\emptyset(n)=\{n(p1-1)(p2-1)(p3-1)\ldots\ldots\ldots\ldots.(pk-1)\}/(p1p2p3\ldots\ldots\ldots pk)$

Example:-
Let G be a cyclic Group, of order o(G)= 12, number of Generators in G=??

Solution:-
Given n=12
Different factors=2*2*3
Distinct Prime number=2,3
Here p1=2 and p2=3, and n=12

Applying langrage's theorem:-

Number of generators in cyclic group=n(p1-1)(p2-1)/p1.p2

=> 12(2-1)(3-1)/2.3

=> 12.1.2/6

=>24/6

=> 4

So number of generators in cyclic group =4

Note:-

1. **Every cyclic group is commutative but vice versa not true.**
2. **Every subgroup of a cyclic group is cyclic.**
3. **Every cyclic group($o(G)=$prime,$o(G)<6$) is an Abelian group converse not true.**
4. **Every group is a Monoid.**

Application of cyclic group

Diffie-Hellman Key Exchange(DHKE)S:-

The Diffie-Hellman key exchange algorithm relies on the properties of cyclic groups. In this protocol, two parties can agree on a shared secret key over an insecure communication channel without directly exchanging the key.

The cyclic group used in Diffie-Hellman is typically a subgroup of a finite field. The security of the algorithm is based on the difficulty of the discrete logarithm problem, which is computationally hard in large cyclic groups.

Elliptic Curve Cryptography (ECC):

Elliptic Curve Cryptography is a type of public-key cryptography that involves the properties of cyclic subgroups of elliptic curves over finite fields.

ECC provides strong security with shorter key lengths compared to traditional methods like RSA. The security of ECC is based on the difficulty of the elliptic curve discrete logarithm problem.

RSA Algorithm (Indirectly):

While the RSA algorithm itself does not directly use cyclic groups, it relies on the difficulty of factoring large composite numbers, which is related to the mathematical properties of certain groups.

The security of RSA is based on the difficulty of factoring the product of two large prime numbers. The mathematical structure of the multiplicative group modulo n (where n is the product of two primes) comes into play, even though it may not be explicitly considered a cyclic group.

In summary, cyclic groups and their properties are crucial in various cryptographic protocols, providing a foundation for secure key exchange and encryption

Thanku