**Algebraic Structure**

A non empty set S is called an algebraic structure w.r.t binary operation (\*) if it follows following axioms:

* **Closure:**(a\*b) belongs to S for all a,b ∈ S.

**Ex :** S = {1,-1} is algebraic structure under \*

As 1\*1 = 1, 1\*-1 = -1, -1\*-1 = 1 all results belongs to S.

But above is not algebraic structure under + as 1+(-1) = 0 not belongs to S.

**Semi Group**

A non-empty set S, (S,\*) is called a semigroup if it follows the following axiom:

* **Closure:**(a\*b) belongs to S for all a,b ∈ S.
* **Associativity:** a\*(b\*c) = (a\*b)\*c ∀ a,b,c belongs to S.

**Note:** A semi group is always an algebraic structure.

**Ex :** (Set of integers, +), and (Matrix ,\*) are examples of semigroup.

**Monoid**

A non-empty set S, (S,\*) is called a monoid if it follows the following axiom:

* **Closure:**(a\*b) belongs to S for all a,b ∈ S.
* **Associativity:** a\*(b\*c) = (a\*b)\*c ∀ a,b,c belongs to S.
* **Identity Element:**There exists e ∈ S such that a\*e = e\*a = a ∀ a ∈ S

**Note:** A monoid is always a semi-group and algebraic structure.

**Ex :** (Set of integers,\*) is Monoid as 1 is an integer which is also identity element .  
(Set of natural numbers, +) is not Monoid as there doesn’t exist any identity element. But this is Semigroup.  
But (Set of whole numbers, +) is Monoid with 0 as identity element.

**Group**

A non-empty set G, (G,\*) is called a group if it follows the following axiom:

* **Closure:**(a\*b) belongs to G for all a,b ∈ G.
* **Associativity:** a\*(b\*c) = (a\*b)\*c ∀ a,b,c belongs to G.
* **Identity Element:**There exists e ∈ G such that a\*e = e\*a = a ∀ a ∈ G
* **Inverses:**∀ a ∈ G there exists a-1 ∈ G such that a\*a-1 = a-1\*a = e

**Note:**

1. A group is always a monoid, semigroup, and algebraic structure.
2. (Z,+) and Matrix multiplication is example of group.

**Abelian Group or Commutative group**

A non-empty set S, (S,\*) is called a Abelian group if it follows the following axiom:

* **Closure:**(a\*b) belongs to S for all a,b ∈ S.
* **Associativity:** a\*(b\*c) = (a\*b)\*c ∀ a,b,c belongs to S.
* **Identity Element:**There exists e ∈ S such that a\*e = e\*a = a ∀ a ∈ S
* **Inverses:**∀ a ∈ S there exists a-1 ∈ S such that a\*a-1 = a-1\*a = e
* **Commutative:** a\*b = b\*a for all a,b ∈ S

**Ring –** Let addition (+) and Multiplication (.) be two binary operations defined on a non empty set R. Then R is said to form a ring w.r.t addition (+) and multiplication (.) if the following conditions are satisfied:

1. (R, +) is an abelian group ( i.e commutative group)
2. (R, .) is a semigroup
3. For any three elements a, b, c  R the left distributive law a.(b+c) =a.b + a.c and the right distributive property (b + c).a =b.a + c.a holds.

Therefore a non- empty set R is a ring w.r.t to binary operations + and . if the following conditions are satisfied.

1. For all a, b  R, a+b R,
2. For all a, b, c  R a+(b+c)=(a+b)+c,
3. There exists an element in R, denoted by 0 such that a+0=a for all a  R
4. For every a  R there exists an y  R such that a+y=0. y is usually denoted by -a
5. a+b=b+a for all a, b  R.
6. a.b  R for all a.b  R.
7. a.(b.c)=(a.b).c for all a, b  R
8. For any three elements a, b, c  R a.(b+c) =a.b + a.c and (b + c).a =b.a + c.a. And the ring is denoted by (R, +, .).

R is said to be a commutative ring if the multiplication is commutative.

**Some Examples –**

1. (, + ) is a commutative group .(, .) is a semigroup. The disrtributive law also holds. So, ((, +, .) is a ring.
2. **Ring of Integers modulo n:** For a n  let  be the classes of residues of integers modulo n. i.e  ={).  
   (, +) is a commutative group ere + is addition(mod n).  
   (, .) is a semi group here . denotes multiplication (mod n).  
   Also the distriutive laws hold. So ((, +, .) is a ring.

Many other examples also can be given on rings like (, +, .), (, +, .) and so on.

Before discussing further on rings, we define **Divisor of Zero in A ring**and the concept of **unit**.

**Divisor of Zero in A ring –**  
In a ring R a non-zero element is said to be divisor of zero if there exists a non-zero element b in R such that a.b=0 or a non-zero element c in R such that c.a=0 In the first case a is said to be a left divisor of zero and in the later case a is said to be a right divisor of zero . Obviously if R is a commutative ring then if a is a left divisor of zero then a is a right divisor of zero also .

**Example –** In the ring (, +, .)  are divisors of zero since  
 and so on .  
On the other hand the rings (, +, .), (, +, .), (, +, .) contains no divisor of zero .

**Units –**  
In a non trivial ring R( Ring that contains at least to elements) with unity an element a in R is said to be an unit if there exists an element b in R such that a.b=b.a=I, I being the unity in R. b is said to be multiplicative inverse of a.

Some Important results related to Ring:

1. If R is a non-trivial ring(ring containing at least two elements ) withunity I then I  0.
2. If I be a multiplicative identity in a ring R then I is unique .
3. If a be a unit in a ring R then its multiplicative inverse is unique .
4. In a non trivial ring R the zero element has no multiplicative inverse .

Now we introduce a new concept Integral Domain.

**Integral Domain –** A non -trivial ring(ring containing at least two elements) with unity is said to be an integral domain if it is commutative and contains no divisor of zero ..

**Examples –**  
The rings (, +, .), (, +, .), (, +, .) are integral domains.  
The ring (2, +, .) is a commutative ring but it neither contains unity nor divisors of zero. So it is not an integral domain.

Next we will go to Field .

**Field –** A non-trivial ring R wit unity is a field if it is commutative and each non-zero element of R is a unit . Therefore a non-empty set F forms a field .r.t two binary operations + and . if

1. For all a, b  F, a+b F,
2. For all a, b, c  F a+(b+c)=(a+b)+c,
3. There exists an element in F, denoted by 0 such that a+0=a for all a  F
4. For every a  R there exists an y  R such that a+y=0. y is usually denoted by (-a)
5. a+b=b+a for all a, b  F.
6. a.b  F for all a.b  F.
7. a.(b.c)=(a.b).c for all a, b  F
8. There exists an element I in F, called the identity element such that a.I=a for all a in F
9. For each non-zero element a in F there exists an element, denoted by  in F such that =I.
10. a.b =b.a for all a, b in F .
11. a.(b+c) =a.b + a.c for all a, b, c in F

**Examples –** The rings (, +, .), (, + . .) are familiar examples of fields.

Some important results:

1. A field is an integral domain.
2. A finite integral domain is a field.
3. A non trivial finite commutative ring containing no divisor of zero is an integral domain

REFERENCES

<http://www.brainkart.com/article/Classical-Encryption-Techniques_8339/>

<https://www.tutorialspoint.com/cryptography/index.htm>

<https://www.geeksforgeeks.org/cryptography-introduction/>

[https://www.techopedia.com/definition/1770/cryptography#:~:text=Cryptography%20involves%20creating%20written%20or,information%20to%20be%20kept%20secret.&text=Information%20security%20uses%20cryptography%20on,transit%20and%20while%20being%20stored](https://www.techopedia.com/definition/1770/cryptography).

<https://www2.slideshare.net/lineking/classical-encryption-techniques-in-network-security?qid=e388c29f-793d-4f2b-bcaf-9d22e9ca07b5&v=&b=&from_search=1>

<https://www.researchgate.net/publication/334418542_A_Review_Paper_on_Cryptography>

<https://www.academia.edu/Documents/in/Cryptography>