JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Topic – "Introduction of Ring theory"

Amrish Kumar Srivastav
Assistant Professor
Department of Mathematics,
Araria College, Araria
Bihar, India

ABSTRACT

In mathematics, rings are algebraic structure that generalizes fields. It is not necessary that multiplication should be commutative and multiplicative inverse exist. In other words, a ring is a set equipped with two binary operation satisfying properties analogous to those of addition and multiplication of integers. Ring element may be numbers such as integers or complex number, but they may also be non numerical objects such as polynomial, square matrix, functions and power series.

KEY WORDS: structure, analogous, fields, polynomial

INTRODUCTION

In 1817, Rechard Dedekind [3] defined the concept of the ring of integers of a number. He introduced the term "ideal" but did not use the term "ring" and concept of ring in general. Rechard Dedekind was a German mathematician who made important contribution to number theory and abstract algebra particularly in ring theory. His best contribution is definition of real numbers which is known as Dedekind cut in mathematics.

The first formal definition of ring was given by Adolf Fraenkel in 1915[1] but his axioms were stricter than those in the modern definition. For Example, he required every non-zero-divisor to have a multiplicative inverse. In 1921, Emmy Noether [2] gave a modern axiomatic definition of commutative rings (with and without 1) and developed the foundations of commutative ring theory but did not include multiplicative identity. Fraenkel included multiplicative identity in ring.

CONCEPT

A ring is an ordered triple (R, +, *) consisting of a non-empty set R and two binary operations on R called addition (+) and multiplication (*), satisfying the following properties:

1- (R, +) is an abelian group, that is,

(a) -Closure law:

$$a + b = b + a, \quad \text{for all } a, b \text{ in } R$$

(b)- Associative law:

$$a + (b + c) = (a + b) + c, \quad \text{for all } a, b, c \text{ in } R$$

(c)- Existence of identity:

There is an element $0 \in R$ satisfying,

$a + 0 = a$, for all a in R.

(d)- Existence of inverse:

For every $a \in R$ there is an element $b \in R$

Such that, $a + b = 0$.

(e)- Commutative law:

$$a + b = b + a, \quad \text{for all } a, b \text{ in } R.$$

2- R is associative under multiplication: i.e.,

$(a * b) * c = a * (b * c)$, for all $a, b, c \in R$.

3- Multiplication is distributive (on both sides) over addition:

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

and $(a + b) * c = a * c + b * c$, for all a, b, c in R.

(These two distributive laws are respectively called the left distributive law and the right distributive law.)

Some common uses in ring:

(1)- We usually refer simply to the ring as R, rather than (R, +, *).

(2)- We usually write a b instead of a*b.

(3)- The identity of the additive Abelian group is called zero element of the ring R and is unique. We denote the zero element of a ring by 0.

(4)- The additive inverse of an element a of the additive Abelian group (R, +, *) shall as usual and denoted by -a. Thus, in a ring R;

$$a + (-a) = 0, \text{ for all } a \in R.$$

(5)- If $a - b \in R$, we denote $a + (-b)$ by $a - b$.

(6)- If a ring R contains only one element, i.e.,

$R = \{ 0 \}$, then it is called a trivial ring or zero ring.

In other words we can define ring as below also:

If (R, +, *) is a ring, then:

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

(2) - (R, *) is semi group.

(3) - The additive identity is unique.

(4) - The additive inverse of any element in R is unique.

(5) - The cancellation law for addition holds.

i.e., if $a, b, c \in R$. with $a + b = a + c$,

$\Rightarrow b = c$

Commutative ring: A commutative ring (R, +, *) is a ring for which $a\,b = b\,a$, for all $a, b \in R$. If a ring is not commutative it is called non commutative.

Ring with unity:

A ring with identity e, which is also called a ring with unity, is a ring R which contains an element $e \in R$ (with e is not equal to zero) satisfying,

$$e\,a = a\,e = a \text{ , for all } a \in R.$$

Generally, the unity or identity element of a ring R is denoted by 1 or 1R.

Finite Ring:

A ring which has finite many elements is called finite ring.

Theorem: Let R be a ring. Then for all $a, b, c \in R$

(1): $a\,0 = 0 = 0\,a$.

(2): $a\,(-b) = -(a\,b) = (-a)\,b$.

(3): $a\,(b - c) = a\,b - a\,c$

and $(a - b)\,c = a\,c - b\,c$.

(4): $(-a) \cdot (-b) = a\,b$.

Proof:

(1): $a\,0 = a\,(0 + 0)$, (since $0 = 0 + 0$)

$= a\,0 + a\,0$ (By left distributive law)

Thus, $a\,0 + (-(a\,0)) = a\,0$

So, $0 = a\,0$

Similarly we can show that 0 = 0 a

Hence a 0 = 0 = 0 a

(2): 0 = a 0

= a (b + (-b))

= a b + a (-b) (By left distributive law)

Thus, - (a b) = a (-b).

Similarly we can show that –

-(a b) = (-a)b

Hence a (-b) = - (a b) = (-a) b.

(3): a (b – c) = a (b + (- c))

= a b + a (-c) (By left distributive law)

= a b – a c.

Similarly, we can show that,

(a – b) c = a c – b c

Hence, a (b – c) = a b – a c

and (a - b) c = a c – b c

(4): (-a) (-b) = -(a (-b)) (by property (2))

= -(-(a b)) (by property (2))

= a b

Definition: Let (R, +, *) be a ring, and S a nonempty subset of R. If (S, +, *) is also a ring under the same operations as R, then S is called a subring of R[4].

In other words, let R be ring. A non empty set S of the set R is said to be a subring of R if s is closed with respect to operations of addition and multiplication in R and S itself is a ring for these operations.

If S is a sub ring of a ring R, it is obvious that S is a subgroup of the additive group of R.

Improper subring:

Every ring R has two trivial sub rings 0 and R itself. These are also known as improper subring.

Example:

(1): (Z, +, *) is a subring of the ring (Q, +, *).

(2): (Q, +, *) is a subring of the ring (R, +, *).

Theorem: Prove that the necessary and sufficient condition for a non empty subset S of a ring R to be a subring of R are,

1- $a \in S, b \in S \Rightarrow a - b \in S$

2- $a \in S, b \in S \Rightarrow a\,b \in S$

Proof: First we prove necessary part.

Let (S, +, *) is subring of (R, +, *).

Since s is a group with respect to addition,

Therefore, $b \in S \Rightarrow -b \in S$

Since S is closed with respect to addition.

Therefore, $a \in S, b \in S \Rightarrow a \in S, -b \in S$

$\Rightarrow a + (-b) \in S$

$\Rightarrow a - b \in S$

Hence the condition is necessary.

Now we prove sufficient part.

Let S is non empty subset of Rand condition (1) and (2) is satisfied.

From eq. (1), we have,

$a \in S, -a \in S \Rightarrow a - a \in S$

$\Rightarrow 0 \in S$

Hence element zero belongs to S.

Now since $0 \in S$, therefore from eq. (1) we have

$0 \in S, a \in S \Rightarrow 0 - a \in S$

$\Rightarrow -a \in S$

$\Rightarrow$ Each element of S possess additive inverse.

Now if $a, b \in S$ then $-b \in S$

Hence from eq. (1) we have

$a \in S, -b \in S \Rightarrow a - (-b) \in S$

$\Rightarrow a + b \in S$

Hence S is closed with respect to addition.

Since S is subset of R. Therefore, associative and commutative law of addition must hold in S. Since, it holds in R.

$\therefore$ (S, +) is an abelian group.

From eq. (2),S is closed with respect to multiplication.

Associativity of multiplication and distributivity of multiplication over addition must hold in S, since they hold in R.

Hence S is subring of R.

Theorem: Prove that the intersection of any two subring of a ring R is a subring of R.

Proof: Let S_1 and S_2 be two subring of a ring R. Then $S_1 \cap S_2$ is non empty.

Thus, $0 \in S_1$, $0 \in S_2$ and hence, $0 \in S_1 \cap S_2$

Since, $S_1 \subseteq R$ and $S_2 \subseteq R$, we have, $S_1 \cap S_2 \subseteq R$ and hence,

$S_1 \cap S_2$ is a non-empty subset of R.

Let $a, b \in S_1 \cap S_2$, thus $a, b \in S_1$ and $a, b \in S_2$

Since S_1 and S_2 are subring of R, we have $a - b, a * b \in S_1$ and $a - b, a * b \in S_2$

This is theorem that non-empty subset S of a ring (R, +, *) is a subring if and only if for all $a, b \in S$ we have $a - b \in S$ and $a * b \in S$.

Then $a - b, a * b \in S_1 \cap S_2$ and hence $S_1 \cap S_2$ is a subring of R of (R, +, *).

Theorem: Prove that the intersection of the family of subring which contain a given subset m of a ring R is the smallest subring containing the subset M.

Proof: Let R is a ring and m is any subset of R. Further we suppose that S is a subring of R

Such that $M \subseteq R$ and T is any subring of R containing M then $S \subseteq T$

Then S is called the subring of R generated by the subset M.

In short we say, If S is the smallest subring of R containing M, and then S is called the subring generated by M.

We shall now introduce another algebraic subsystem of a ring called ideal which is more special than subring. The ideal of a ring and normal subgroup of a group are quite parallel.

Definition:

Left ideal: A non empty set S of a ring R is said to be a left ideal of R if

1- S is subgroup of R with respect to addition.

2- $r s \in S$ for all $r \in R$ and for all $s \in S$

Right ideal: A non empty set S of a ring R is said to be a left ideal of R if,

1- S is subgroup of R with respect to addition.

2- $s r \in S$ for all $r \in R$ and for all $s \in S$

Ideal: Let (R, +, *) be a ring. Then (S, +, *0) is an ideal of (R, +, *). if and only if-

1- $a, b \in S \Rightarrow a + (-b) \in S$

2- $s \in S$ and $r \in R \Rightarrow r s \in S$ and $s r \in S$ for all $r \in R$ and for all $s \in S$

Another definition of idea: A subset S of a ring R is called an ideal of R. If

1- S is a subgroup of the additive group R and

2- $s \in S$ and $r \in R \Rightarrow r s \in S$ and $s r \in S$ for all $r \in R$ and for all $s \in S$

If R is a commutative ring, then every left ideal also be right ideal. Hence in commutative ring every left or right ideal is an ideal.

Every ring always possess two improper ideals one R itself and the other consisting of 0 only. Any other ideals are called proper ideals.

Simple Ring: A ring having no proper ideals is called a simple ring.

Theorem: Prove that every ideal is a subring.

Proof: Let (R, +,*) is a ring and (S, +,*) be an ideal in (R, +,*).

Hence it is given that-

1- $a, b \in S \Rightarrow a + (-b) \in S$

2- $a \in S$ and $r \in R \Rightarrow r\,a \in S$ and $a\,r \in S$ for all $r \in R$ and for all $a \in S$

For showing S is a subring of R we have to show that

(i)- $a, b \in S \Rightarrow a + (-b) \in S$

(ii)- $a \in S, b \in S \Rightarrow a\,b \in S$

It is clear that condition (1) and (i) is same. Hence, now we have to prove only condition (ii).

Let $a \in S, b \in S$

Since S is subset of R.$\Rightarrow b \in S$

Hence by condition (2) we get $a \in S, b \in S \Rightarrow a\,b \in S$

Since both the condition (i) and (ii) is satisfied. Hence theorem is proved.

Converse of this theorem is not true. i.e., there are many sub rings which are not ideals. Some example of such type of subring is given below.

Example: The set Q of rational numbers with usual operation of addition and multiplication is a commutative ring.

The set I of integers is a subset of Q and is a commutative ring.

Hence I is subset of Q but I is not an ideal of Q. Because we can find an integer $a \in I$ and one rational number $r \in Q$ such $a\,r \notin I$

For example: let a = 1 and r =1/2 and we take,

$a\,r = 1 \times 1/2 = 1/2 \notin I$

Theorem: Prove that intersection of two ideals in a ring is also an ideal in the ring [5].

Proof: Suppose S_1 and S_2 be two ideals in a ring R.

Let $S = S_1 \cap S_2$

Since every ideal is a subring, therefore each of S_1 and S_2 is a subring.

We know that intersection of two sub rings is a subring.

Therefore $S_1 \cap S_2 = s$ is a subring.

Thus in order to prove that s is an ideal. We need to show that

$a \in S$ and $r \in R \Rightarrow a\,r \in S$

Since $a \in S$, therefore $a \in S_1$ and $a \in S_2$

Also $a \in S_1$ and $r \in R \Rightarrow a\,r \in S_1$

(Because S_1 is an ideal)

Similarly $a \in S_2$ and $r \in R \Rightarrow a\,r \in S_2$

(Because S_2 is an ideal)

Hence $a\,r \in S_1 \cap S_2 \Rightarrow a\,r \in S$

Similarly we can prove $r\,a \in S$

Hence S is an ideal in R.

Theorem: Prove that intersection of any collection of ideals in a ring is also an ideal in the ring.

Proof: Suppose R be a ring and let $S = \cap S_\alpha$

Since every ideal is a subring.

Hence each of S_α is a subring.

We know that the intersection of arbitrary collection of subring is a subring.

Therefore $\cap S_\alpha = S$ is a subring.

Now let $a \in S_\alpha$ for a fixed α and $r \in R$

Since S_α is an ideal in R

Hence $a\,r \in S_\alpha$ for each α

$\Rightarrow a\,r \in \cap S_\alpha$ for each α

$\Rightarrow a\,r \in S$

Similarly it can be shown that $r\,a \in S$

Hence S is an ideal in r.

Proposition: Let R be a ring with identity 1 and let I be a left (respectively right) ideal of a ring R. Then I is a proper left (respectively right) ideal of R iff $1 \neq I$.

Proof: Suppose that I is a proper left ideal of R. Thus there is $r \in R$ with $r \notin I$.

Assume that $1 \in I$, then $r = r.1 \in I$ and this is a contradiction.

Thus, $1 \neq I$, Suppose that $1 \neq I$, thus I R and hence I is a proper left ideal of R.

Proposition: Let R be a ring and let a be an element of R.

Then $Ra = \{ r\,a \mid r \in R \}$ is a left ideal of R.

Proof: Since $0 = 0.\,a$, we have $0 \in Ra$ and hence

$\varnothing \neq Ra \subseteq R$, Let $x\,.\,y \in R\,a$ and $r \in R$

Thus $x = s_1 a$ and $y = s_2 a$, for some $s_1 \cap s_2 \in R$.

Then, $x - y = s_1\,a - s_2\,a$

$= (s_1 - s_2)\,a \in Ra$ and

$r\,x = r(s_1 a)$

$= (r\ s_1)\ a \in Ra$

Hence $Ra = \{ r\ a \mid r \in R \}$ is a left ideal of R.

Prime Ideal:

Definition: Let R be a ring and n is an ideal in R. If, N has the property that when $a\ b \in N$ then either $a \in N$ or $b \in N$, then N is called a prime ideal.

Example: We consider the ideal $\{5\} = \{0, \pm5, \pm10, \pm15, \ldots\}$ in ring of integers I.

In the above ideal, if $a\ .\ b \in 5$, Then either a is a multiple of 5 or b is multiple of 5 i.e., either $a \in \{5\}$, or $b \in \{5\}$

Hence {5} is prime ideal.

CONCLUSION

Ring is algebraic structure with two binary operation.

It obeys some definite laws such as closure law, associative law, existence of identity, existence of inverse, commutative law and multiplication associative and distributive. Its properties are interesting and useful in solving many problems. A sub ring of ring R is subset of the ring R and ideal of a ring is special subset of its its element.

ACKNOWLEDGEMENT

I would like to express my special thanks of gratitude to my guide Dr M. K. Manoranjan as well as my colleague who encourage me for writing paper for publishing. I am really thankful to them. Secondly, I would also like to thank my parents and friends who helped me a lot in finishing paper writing within the short time. Just because of them I am able to write this paper and make it good and enjoyable experience.

References

1- Fraenkel, A. (1915), "**Über die Teiler der Null und die Zerlegung von Ringen**". J. Reine Agew.Math.1915 (145) :139176.doi:10.1515/crll. 1915. 145. 139. S2CID 118962421

2- Dick, Asuguste , Emmy Noether, , translated by Blocher, H.I.,Birkhäuser,
ISBN 3-7643-3019-8, p. 44–45

3-Pierce, Richard S. (1982), "**Associative Algebras"**, Graduate Texts in Mathematics, vol. 88, New York: Springer-Verlag,
ISBN 0-387-90693-2, MR 067465

4- Iain T. Adamson (1972), " **Elementary rings and modules"**, University Mathematical Texts, Oliver and Boyd. pp. 14–16. ISBN 0-05-002192-3

5- Hazewinkel, Michiel, Gubareni, Nadiya, Gubareni, Nadezhda, Mikhaĭlovna, Kirichenko, Vladimir V (2004), "**Algebras, ringsand modules"** Vol. 1 Springer. ISBN 1-4020-2690-0