Dr. O. P. Raman
Dept of Mathematics

For T.D.C. Part II
Paper - 3

Abstract (Modern) Algebra

RING ①

Definition

Let R be a set and let two binary operations called addition (denoted by +) and multiplication (denoted by ·) be defined over the set R. Then the system $(R, +, \cdot)$ is called a ring R if the following postulates are satisfied.

I. Laws of addition :

(i) $a + b \in R$; $a, b \in R$

(ii) $(a + b) + c = a + (b + c)$; $a, b, c \in R$ (associative law)

(iii) There exists an element 0 in R called zero of the ring such that $a + 0 = 0 + a = a$ for every $a \in R$.

(iv) For each element a in R there exists $-a$ in R called the negative of a such that

$$a + (-a) = -a + a = 0.$$

(v) $a + b = b + a$; $a, b \in R$ (commutative law)

II. Laws of multiplication :

(i) $a \cdot b \in R$, $a, b \in R$

(ii) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$; $a, b, c \in R$ (associative law)

III. Distributive laws :

(i) $a \cdot (b + c) = a \cdot b + a \cdot c$

(ii) $(b + c) \cdot a = b \cdot a + c \cdot a$; $a, b, c \in R$.

Another form of definition : From the laws of addition it is clear that a ring is an Abelian group with respect to addition.

Thus we can define a ring as follows :

A set R with two binary operations called addition and multiplication is said to be a ring if the following postulates are satisfied.

(3)

3.3 Uniqueness of Zero Element

To prove that the zero element of a ring is unique. (RU 1979)

Proof. If possible let the ring R has two zero elements 0 and 0'. Then by definition of zero element we get

$$a+0=a$$

$$a+0'=a \quad \ldots (1)$$

for all $a \in R$. $\quad \ldots (2)$

But $0' \in R$. So by (1), $0'+0=0'$.

Also $0 \in R$. So by (2), $0+0'=0$.

Again $0'+0=0+0'$, (by commutative law for addition).

$\therefore \quad 0'=0$.

This proves that the ring has unique zero element.

3.4 Uniqueness of Additive Inverse

To prove that the additive inverse of an element of a ring is unique.

Proof. Let, if possible, b and b' are two additive inverses of $a \in R$, the ring.

(4)

$$a+b=0$$

Then

$$a+b'=0$$

$\Rightarrow a+b=a+b'$

$\Rightarrow (-a)+(a+b)=(-a)+(a+b')$

$\Rightarrow \{(-a)+a\}+b=\{(-a)+a\}+b'$, by associative law for addition

$\Rightarrow 0+b=0+b'$

$\Rightarrow b=b'$.

This proves that, in a ring R, the inverse of all element is unique.

3.5 Cancellation Laws

In a ring $(R, +, .)$ if a, b, c are any three elements then

(i) $a+b=a+c \Rightarrow b=c$ *(left cancellation)*

(ii) $b+a=c+a \Rightarrow b=c$ *(right cancellation).*

Proof. As R is a ring under '+' and '.' we have for every $a \in R$ these exists $-a \in R$ such that

$$a+(-a)=(-a)+a=0.$$

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

$\Rightarrow (-a)+(a+b)=(-a)+(a+c)$

$\Rightarrow \{(-a)+a\}+b=\{(-a)+a\}+c$,

by associative law for addition

$\Rightarrow 0+b=0+c$

$\Rightarrow b=c$.

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

$\Rightarrow a+b=a+c$, by commutative law for addition.

Then as in (1) we can prove that $b=c$.

(c)

Taking $-b$ for b we get

$$a.\{-(-b)\}=-\{a.(-b)\}$$

$$\Rightarrow a.b=-\{a.(-b)\}.$$

Again from (ii) we get

$$-(a.b)=(-a).b. \quad \cdots (1)$$

Taking $-b$ for b we get

$$-\{a.(-b)\}=(-a).(-b).$$

$\therefore$ From (1) and (2), $(-a).(-b)=a.b.$ $\cdots$ (2)

(iv) $a.(b-c)=a.\{b+(-c)\}$

$=a.b+a.(-c)$, {by distributive law}

$=a.b+\{-(a.c)\}$,

{$\because$ by (ii), $a.(-c)=-(a.c)$}

$=a.b-a.c.$

(v) $(b-c).a=\{b+(-c)\}.a$

$=b.a+(-c).a$, {by distributive law}

$=b.a+\{-(c.a)\}$,

{$\because$ by (ii), $(-c).a=-(c.a)$}

$=b.a-c.a.$

3.8 Uniqueness of Unity in a Ring with Unity

To prove that the unity, if it exists in a ring, is unique.

(Mlth U 1981)

Proof. If possible let $e, e' \in R$ are two unity elements in the ring $(R, +, .)$ with unity.

If we prove $e=e'$ our proposition is established.

Now $a.e=e.a=a$ for all $a \in R$

and $a.e'=e'.a=a$ for all $a \in R$.

$\therefore$ As $e' \in R$, $e'.e=e.e'=e'$.

As $e \in R$, $e.e'=e'.e=e$.

Thus $e'=e$.

$\therefore$ Unity in a ring is unique, if it exists.

3.9 Divisors of Zero in a Ring

If in a ring $(R, +, .)$ we have

$$ab=0 \text{ where } a, b \in R \text{ and } a \neq 0, b \neq 0$$

then we say a is a *left-divisor of zero* and b is a *right-divisor of zero.*

An element a which is a left-divisor as well as a right-divisor is called a *divisor of zero.*

Clearly in a commutative ring every left-divisor of zero as well as a right-divisor of zero is a divisor of zero.

(B) *If* $(R, +, .)$ *is a ring then to prove that*

(i) $a \cdot 0 = 0 \cdot a = 0$,

(ii) $a \cdot (-b) = -(a \cdot b) = (-a) \cdot b$, (BU 1979; Mith U '79; MU '86)

(iii) $(-a) \cdot (-b) = a \cdot b$, (BU 1979; Mith U '79; MU '86)

(iv) $a \cdot (b-c) = a \cdot b - a \cdot c$, (BU 1979); (MU 1988)

(v) $(b-c) \cdot a = b \cdot a - c \cdot a$

where $a, b, c \in R$.

Proof. (i) We have $a \cdot (a+0) = a \cdot a$

{$\because$ $a+0=a$ by existence law of zero element in a ring}.

Also by distributive law,

$$a \cdot (a+0) = a \cdot a + a \cdot 0.$$

$\therefore$ From these, we get

$$a \cdot a + a \cdot 0 = a \cdot a$$

or

$$a \cdot a + a \cdot 0 = a \cdot a + 0,$$

(by the existence of the identity element)

$\therefore$ By cancellation law, $a \cdot 0 = 0$.

Again $(0+a) \cdot a = a \cdot a$, {$\because$ $0+a=a+0=a$}

or $0 \cdot a + a \cdot a = a \cdot a$, by distributive law

or $0 \cdot a + a \cdot a = 0 + a \cdot a$,

(by the existence of the identity element)

$\therefore$ By cancellation law, $0 \cdot a = 0$.

Thus $a \cdot 0 = 0 \cdot a = 0$.

(ii) $a \cdot b + a \cdot (-b) = a \cdot \{b + (-b)\}$, using distributive law

$= a \cdot 0$, (by the existence of the inverse element)

$= 0$, by (i).

$\therefore$ $a \cdot (-b)$ is the inverse element of $a \cdot b$

i.e. $a \cdot (-b) = -(a \cdot b)$.

Again $a \cdot b + (-a) \cdot b = \{a + (-a)\} \cdot b$,

using distributive law

$= 0 \cdot b$

(by the existence of the inverse element)

$= 0$, by (i).

$\therefore$ $(-a) \cdot b$ is the inverse element of $a \cdot b$

i.e. $(-a) \cdot b = -(a \cdot b)$

Thus we get $a(-b) = -(a \cdot b) = (-a) \cdot b$.

(iii) From (ii) we have

$$a \cdot (-b) = -(a \cdot b).$$

(7)

8. *To prove that a ring R is without divisor of zero if and only if the cancellation laws for multiplication hold in R.* **(MU 1980 H '85; RU '87)**

Proof. Let R be a ring without divisor of zero under the operations '+', '.'.

$\therefore \; a \,.\, b=0 \Rightarrow$ either $a=0$ or $b=0$.

$\therefore$ If $a \neq 0$, $a \,.\, b=0 \Rightarrow b=0$. .. (1)

Now $a \,.\, (b-c)=a \,.\, b-a \,.\, c$ {by property B(iv), § 3.7}.

$\therefore \; a \,.\, b=a \,.\, c \Rightarrow a \,.\, b-a \,.\, c=0$

$\Rightarrow a \,.\, (b-c)=0$

$\Rightarrow b-c=0$, by (1)

$\Rightarrow b-c+c=0+c$

$\Rightarrow b=c$. .. (2)

Again $(b-c) \,.\, a=b \,.\, a-c \,.\, a$. .. (3)

If $b \neq 0$, $a \,.\, b=0 \Rightarrow a=0$.

$\therefore \quad b \,.\, a = c \,.\, a \Rightarrow b \,.\, a - c \,.\, a = 0$

$\Rightarrow (b-c) \,.\, a = 0$, by (2)

$\Rightarrow b - c = 0$, by (3)

$\Rightarrow b - c + c = 0 + c$

$\Rightarrow b = c.$

Thus cancellation laws of multiplication hold for the ring.

(1) R is an Abelian group with respect to addition;

(2) The closure law and the associative law for multiplication are satisfied, that is,

(i) $a \cdot b \in R$, $a, b \in R$

(ii) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$; $a, b, c \in R$

(3) The distributive laws w.r.t. addition and multiplication are satisfied; that is,

(i) $a \cdot (b + c) = a \cdot b + a \cdot c$

(ii) $(b + c) \cdot a = b \cdot a + c \cdot a$; $a, b, c \in R$.

(A) Commutative Ring : Definition : A ring R is said to be *commutative* if

$$a \cdot b = b \cdot a; \; a, b \in R$$

It means that the set R to be a commutative ring must satisfy in addition to the three laws listed above, the commutative law for multiplication as well.

(B) Ring with Unity : If there exists an element 1 in R such that $a \cdot 1 = 1 \cdot a = a \; \forall \; a \in R$ then the ring R is called a *ring with unity element 1*.

A ring which is commutative and possesses an unity element is called a *commutative ring with unity.*