Department of Distance Education
Punjabi University, Patiala

Lesson No. :

SECTION : B

B.A. PART–III **MATHEMATICS : PAPER I**
(SEMESTER - V) **ABSTRACT ALGEBRA**

LESSON NO. 2.1 **AUTHOR : DR. CHANCHAL**

RINGS – I

Objectives

I. Introduction
II. Zero Divisor and Integral Demain
III. Division Ring and Field
IV. Subrings
V. Centre of the Ring
VI. Characteristic of a Ring
VII. Idempotent and Nilpotent elements.
VIII. Product of Rings
IX. Self Check Exercise

I. Introduction

Definition : A non empty set R, together with two binary compositions + and $\sqcup$ is said to form a Ring if the following axioms are satisfied:

(i) $a + (b + c) = (a + b) + c$ for all $a, b, c \in R$

(ii) $a + b = b + a$ for $a, b \in R$

(iii) $\exists$ some element 0(called zero) in R, s.t., $a + 0 = 0 + a = a$ for all $a \in R$

(iv) for each $a \in R$, $\exists$ an element $(-a) \in R$, s.t., $a + (-a) = (-a) + a = 0$

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

(vi) $a. (b + c) = a. b + a . c$

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

Remarks : (a) Since we say that + and $\sqcup$ are binary compositions on R, it is understood that the closure properties w.r.t. these hold in R. In other words, for all $a, b \in R$, $a + b$ and $a. b$ are unique in R.

(b) One can use any other symbol instead of +and ., but for obvious reasons, we use these two symbols.

(c) Axiom (v) is named associativity w.r.t (.) and axiom (vi) is referred to as distributivity (left and right) w.r.t + and $\sqcup$.

(d) Axioms (i) to (iv) could be restated by simply saying that < R, + > forms an abelian group.

(e) Since 0 in axiom (iii) is identity w.r.t +, it is clear that this element is unique.

Definition (Commutative ring) : A ring R is called a commutative ring if ab = ba for all a, b $\in$ R. Again if $\exists$ an element e $\in$ R s.t.,

ae = ea = a for all a $\in$ R

We say, R isa ring with unity. Unity is generally denoted by 1. (It is also called unit element or multiplicative identity)

Note : If unity exists in a ring then it must be unique.

Remark : We recall that in a group by a^2 we meant a. a where '.' was the binary composition of the group. We continue with the same notation in rings as well. In fact, we also introduce similar notation for addition, and write na to mean a + a + ...+ a (n times), n being an integer.

Example 1 : Sets of real numbers, rational numbers, integers form rings w.r.t usual addition and multiplication. These are all commutative rings with unity.

Example 2 : Set E of all even integers forms a commutative ring, without unity (under usual addition and multiplication).

Example 3 : (a) Let M be the set of all 2 × 2 matrices over integers under matrix addition and matrix multiplication. It is easy to see M forms a ring with unity $\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$, but is not commutative.

(b) Let M be set of all matrices of the type $\begin{bmatrix}a & b\\ 0 & 0\end{bmatrix}$ over integers under matrix addition and multiplication. Then M forms a non commutative ring without unity.

Example 4 : The set Z_7 = {0, 1, 2, 3, 4, 5, 6} forms a ring under addition and multiplication modulo 7. (In fact, we could take n in place of 7).

Example 5 : The set R = {0, 4, 6} under addition and multiplication modulo 6 forms a commutative ring with unity. The composition tables are

$\oplus$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

$\otimes$	0	2	4
0	0	0	0
2	0	4	2
4	0	2	4

Since 0 $\otimes$ 4 = 0, 2 $\otimes$ 4 = 2, 4 $\otimes$ 4, we notice 4 is unity of R.

Example 6 : Let F be the set of all continuous functions f : R $\to$ R, where R = set of real numbers. Then F forms a ring under addition and multiplication defined by:

For any f, g $\in$ F

$(f + g)x = f(x) + g(x)$, for all $x \in R$

$(f\ g)x = f(x)\ g(x)$ for all $x \in R$

Example 7 : Let R = {0, a, b, c}, Define + and . on R by

+	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

.	0	a	b	c
0	0	0	0	0
a	0	a	b	c
b	0	a	b	c
c	0	0	0	0

Then one can check that R forms a non commutative ring without unity. In fact it is an example of the smallest non commutative ring.

Theorem 1 : In a ring R, the following results hold

(i) $a.\ 0 = 0.\ a = 0$ for all $a \in R$

(ii) $a(-b) = (-a)b = -ab$ for all $a, b \in R$

(iii) $(-a)(-b) = ab\ \forall\ a, b \in R$

(iv) $a(b - c) = ab - ac.\ \forall\ a, b, c \in R$

Proof : (i) $a.\ 0 = a.\ (0 + 0)$

$\Rightarrow a.\ 0 = a.\ 0 + a.\ 0$

$\Rightarrow a.\ 0 + 0 = a.\ 0 + a.\ 0$

$\Rightarrow 0 = a.\ 0$ (using cancellation w.r.t + in the group < R, + >)

(ii) $a.\ 0 = 0$

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

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

$\Rightarrow a(-b) = -\ (ab)$

Similarly $(-a)b = -ab$.

(iii) $(-a)(-b) = -[a(-b)] = -[-ab] = ab$

(iv) $a(b - c) = a(b + (-c)$

$= ab + a(-c)$

$= ab - ac.$

Remarks : (i) If R is a ring with unity and 1 = 0, then since for any $a \in R$, $a = a.1 = a.0 = 0$, we find R = {0} which is called the trivial ring. We generally exclude this case and thus whenever, we say R is a ringh with unity, it will be understood that $1 \neq 0$ in R.

(ii) If m, n are integers and a, b are elements of ring, then

$n(a + b) = na + nb$

$(n + m)a = na + ma$

$(nm)a = na + ma$

$(nm)a = n(ma)$

$a^m a^n = a^{m+n}$

$(a^m)^n = a^{mn}$

Problem 1 : Let <R, +, .> be a ring where the group <R, +> is cyclic. Show that R is a commutative ring:

Solution : Let <R, + > be generated by a. Let x, y ∈ R be any two elements,. then x = ma, y = na for some integers m, n.

Now xy = (ma)(na)

= (a + a + ...+a)(a + a + ... + a)

m times n times

$= (mn)a^2 = (nm)a^2 = (na)(ma) = yx$

II. Zero Divisor and Integral Demain

We have many times used this property that whenever ab = 0 then either a = 0 or b = 0 that may not always be true. Indeed in the ring of integers (or reals or rationals) this property holds. But if we consider the ring of 2 × 2 matrices over integers, we notice, we can have two non zero elements

A, B s.t, AB = 0, but A ≠ 0 B ≠ 0. In fact, take $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} and B = \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix}$ then A ≠ 0, B ≠ 0. But $AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. In continuation to this, we define.

Definition (Zero-Divisor) : Let R be a ring. An element 0 ≠ a ∈ R is called a zero-divisor, if ∃ an element 0 ≠ b ∈ R s.t., ab = 0 or ba = 0.

Definition (Integral Domain) : A commutative ring R is called an Integral domain if ab = 0 in R ⇒ either a = 0 or b = 0. In other words, a commutative ring R is called an integral domain if R has no zero divisors.

An obvious example of an integral domain is <Z, +, .> the ring of integers whereas the ring of matrices, talked about above is an example of a ring which is not an integral domain. Again, Z × Z will not be an integral domain.

Theorem 2 : A commutative ring R is an integral domain iff for all a, b, c, c ∈ R (a ≠ 0) ab = ac ⇒ b = c.

Proof : Let R be an integral domain

Let ab = ac (a ≠ 0)

Then ab – ac = 0

⇒ a(b – c) = 0

⇒ a = 0 or b – c = 0

since a ≠ 0, we get b = c.

Conversely, let the given condition hold.

i.e. a, b $\in$ R be any elements with $a \neq 0$.

Suppose $ab = 0$

then $ab = a.0$

$\Rightarrow$ $b = 0$ using given condition

Hence $ab = 0 \Rightarrow b = 0$ whenever $a \neq 0$ or that R is an integral domain.

Remark : A ring R is said to satisfy left concellation law if for all a, b, c $\in$ R, $(a \neq 0)$, $ab = ac \Rightarrow b = c$.

Similarly we can talk of right concellation law. It might, of course, be noted that cancellation is of non zero elements only.

Definition (Unit) : An element a in a ring R with unity, is called invertible (or a unit) w.r.t. multiplication if $\exists$ some b $\in$ R such that $ab = 1 = ba$.

Note that, unit and unit element (unity) are different concepts and should not be confused with each othen.

III. Division Ring and Field :

Definition (Division Ring): A ring R with unity is called a Division ring or a skew field if non zero elements of R form a group w.r.t multiplication.

In other words, a ring R with unity is a Division ring if non zero elements of R have multiplicative inverse.

Definition (Field) : A commutative division ring is called a field.

Real numbers form a field, whereas integers do not, under usual addition and multiplication.

Since a division ring (field) forms groups w.r.t two binary compositions, it must contain two identity elements 0 and 1 (w.r.t. addition and multiplication) and thus a division ring (field) has at least two elements.

Example 1: A division ring which is not a field. Let M be the set of all 2 × 2 matrices of the type $\begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix}$ where a, b are complex numbers and $\bar{a}, \bar{b}$ are their conjugates, i.e., if $a = x + iy$, then $\bar{a} = x - iy$. Then M is a ring with unity $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ under matrix addition and matrix multiplication.

Any non zero element of M will be $\begin{bmatrix} x+iy & u+iv \\ -(u-iv) & x-iy \end{bmatrix}$

where x, y, u, v are not all zero.

One can check that the matrix $\begin{bmatrix} \frac{x-iy}{k} & -\frac{u+iv}{k} \\ \frac{(u-iv)}{k} & \frac{x+iy}{k} \end{bmatrix}$

where $k = x^2 + y^2 + u^2 + v^2$, will be multiplicative inverse of the above non zero matrix, showing that M is a division ring. But M will not be a field as it is not commutative as

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}$$

But $$\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}$$

Example 2 : Consider

D = {a + bi + cj + dk| a, b, c, d ∈ R} with $i^2 = j^2 = k^2 = -1$, then D forms a ring.

Two elements a + bi + cj + dk and a' + b'i + c'j + d'k are equal iff' a = a', b = b', c = c', d = d'.

Addition and multiplication of D are defined by

(a + bi + cj + dk) + (a' + b'i + c'j + d'k) = (a + a') + (b + b')i + (c + c')j + (d + d') k and

(a + bi + cj + dk) (a' + b'i + c'j + d'k) = (aa' – bb' – cc' – dd') + (ab' + ba' + cd' – dc') i + (ac' – bd' + ca' – db')j + (ad' + bc' – ab' + da') k

The symbol + in the elements of D is just a notation and is not to be confused with addition in real nmumbers. We identify element o + 1i + oj + ok by i and so on

Thus since i = 0 + li + 0j + 0k

j = 0 + 0i + 1j + 0k

We have ij = k, ji = –k, etc., In fact that shows that D is non commutative. D has unity 1 = 1 + 0i + 0j + 0k

If a + bi + cj + dk be any non zero element of D (i.e., at least one of a, b, c, d is non zero)

then (a + bi + cj + dk) $\frac{(a-bi-cj-dk)}{a^2+b^2+c^2+d^2} = 1$

Hence D is a division ring but not a field.

The elements of D can also be written as quadruples (a, b, c, d)

This ring D is called the ring of quaternions.

Theorem 3 : A field is an integral domain.

Proof : Let < R, +, . > be a field, then R is a commutative ring.

Let ab = 0 in R. We want to show either a = 0 or b = 0. Suppose $a \neq 0$, then a^{-1} exists (definition of field)

Thus $ab = 0$

$\Rightarrow a^{-1}(ab) = a^{-1}0$

$\Rightarrow b = 0$

which shows that R is an integral domain.

Remark : Similarly we can show that a division ring is an integral domain and thus has no zero divisions.

Theorem 4 : A non zero finite integral domain is a field.

Proof : Let R be a non zero finite integral domain.

Let 'R' be the subset of R containing non zero elements of R.

Since associativity holds in R, it will hold in R'. Thus R' is a finite semi group.

Again cancellation laws hold in R (for non zero elements) and therefore, these hold in R'.

Hence R' is a finite semi group w.r.t multiplication in which cancellation laws hold.

$\therefore$ <R', .> forms a group. Note that closure property holds in R' as R is an integral domain.

In other words <R, +, .> is field (being commutative as it is an integral domain)

Aliter : Let $R = \{a_1, a_2, \ldots\ldots, a_n\}$ be a finite non zero integral domain. Let $0 \neq a \in R$ be any element then $aa_1, aa_2, \ldots\ldots, aa_n$ are all in R and if $aa_i = aa_j$ for some $i \neq j$, then by cancellation, we get $a_i = a_j$ which is not true. Hence $aa_1, aa_2, \ldots\ldots, aa_n$ are distinct members of R.

Since $a \in R$, $a = aa_i$ for some i

Let $x \in R$ be any element, then $x = aa_j$ for some j

Thus $ax = (aa_i)x = a(a_ix)$

i.e., $x = a_ix$

Hence, using commutativity we find

$$x = a_ix = xa_i$$

or that a_i is unity of R. Let $a_i = 1$

Thus for $1 \in R$, since $1 = aa_k$ for some k

We find a_k is multiplicative inverse of a. Hence any non zero element of R has multiplicative inverse or that R is a field.

For Example : An infinite integral domain which is not a field is the ring of integers.

Definition : A ring R is called a Boolean ring if $x^2 = x$ for all $x \in R$.

For Example : The ring {0, 1} under addition and multiplication mod 2 forms a Boolean ring.

Problem 2 : Show that a Boolean ring is commutative.

Solution : Let a, b $\in$ R be any elements

Then $a + b \in R$ (closure)

By given condition

$(a + b)^2 = a + b$

$\Rightarrow$ $a^2 + b^2 + ab + ba = a + b$

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

$\Rightarrow$ $ab + ba = 0$

$\Rightarrow$ $a(ab) = - ba$ ...(1)

$\Rightarrow$ $a(ab) = a(-ba)$

$\Rightarrow$ $a^2b = -aba$

$\Rightarrow$ $ab = -aba$ ...(2)

Again (1) gives

$(ab)a = (-ba)a$

$\Rightarrow$ $aba = -ba^2 = -ba$ ...(3)

(2) and (3) give

$ab = ba (= -aba)$

or that R is commutative.

Problem 3 : If in a ring R, with unity , $(xy)^2 = x^2y^2$ for all x, y $\in$ R then show that R is commutative.

Solution : Let x, y $\in$ R be any elements

then $y + 1 \in R$ as $1 \in R$

By given condition

$(x(y + 1))^2 = x^2(y + 1)^2$

$\Rightarrow$ $(xy + x)^2 = x^2(y + 1)^2$

$\Rightarrow$ $(xy)^2 + x^2 + xyx + xxy = x^2(y^2 + 1 + 2y)$

$\Rightarrow$ $x^2y^2 + x^2 + xyx + xxy = x^2y^2 + x^2 + 2x^2y$

$\Rightarrow$ $xyx = x^2y$ ...(1)

Since (1) holds for all x, y in R, it holds for x + 1, y also. Thus replacing x by x + 1, we get

$(x + 1)\, y(x + 1) = (x + 1)^2y$

$\Rightarrow (xy + y)(x + 1) = (x^2 + 1 + 2x)y$

$\Rightarrow xyx + xy + yx + y = x^2y + y + 2xy$

$\Rightarrow yx = xy$ using (1)

Hence R is commutative.

IV. Subrings

Definition : A non empty subset S of a ring R is said to be a subring of R if S forms a ring under the binary compositions of R.

For Example : The ring <z, +, .> of integers is a subring of the ring <R, +, .> of real numbers.

Remarks : 1. The subring of a integral domain will be an integral domain.

2. If R is a ring, then {0} and R are always springs of R, called trivial subrings of R.

Theorem 5 : A non empty subset S of a ring R is a subring of R iff $a, b \in S \Rightarrow ab, a - b \in S$.

Proof : Let S a subring of R

then $a, b \in S \Rightarrow ab \in S$ (closure)

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

as < S, + > is a subgroup of <R, +>.

Conversely, since $a, b \in S \Rightarrow a - b \in S$, we find < S, + > forms a subgroup of <R, +>. Again for any $a, b \in S$, since $S \subseteq R$

$a, b \in R$

$\Rightarrow a + b = b + a$

and so we find S is abelian.

By a similar argument, we find that multiplicative associativity and distributivity hold in S. In other words, S satisfies all the axioms in the definition of ring.

Hence S is a subring of R.

Definition (Subfield) : A non empty subset S of a field F is called a subfield, if S forms a field under the operations in F. Similarly, we can define a subdivision ring of a division ring.

One can prove that S will be a subfield of F iff $a, b \in S, b \neq 0 \Rightarrow a - b, ab^{-1} \in S$.

We may also notice here that a subfield always contains at least two elements, namely 0 and 1 of the field.

Sum of Two Subrings

Definition : Let S and T be two subrings of a ring R. We define

$S + T = \{s + t \mid s \in S, t \in T\}$

then clearly S + T is a non void subset of R. Indeed $0 = 0 + 0 \in S + T$.

Note : Sum of two subrings may not be a subring.

Take the ring M of 2×2 matrices over integers.

Let S = set of all matrices of the type $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$ a, b integers, and

T = set of all matrices of the type $\begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix}$, x an integer.

Then S and T are subrings of M.

Also, S + T would have members of the type $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} + \begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix}$

i.e., matrices of the type $\begin{bmatrix} a & c \\ b & 0 \end{bmatrix}$

That S + T does not form a subring follows from the fact that closure w.r.t. multiplication does not hold, as

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 2 & 2 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 4 & 2 \\ 2 & 2 \end{bmatrix} \notin S + T$$

Definition : Let S be a subset of a ring R, then the smallest subring of R containing S is called the subring generated by S.

Since intersection of subrings is a subring, it is clear that the subring generated by a subset S of R will be the intersection of all subrings of R, containing S. We denote it by < S>. Clearly then <S> = {0} if S = φ . One can show that

$$<S> = \left\{\sum n_i x_1 x_2 \ldots x_n \mid n_i \in Z, x_i \in S\right\}$$

In particular if x ∈ R be an element, then the subring generated by x is the smallest subring of R containing x. It will be the intersection of all subrings of R, containing x. This is denoted by <x>. One can show that' $< x >= \left\{ \sum_{i=0}^{\text{finite}} m_i x^i \mid m_i \in Z \right\}$

V. Centre of the Ring

Definition : Let R be a ring, the set

$$Z(R) = \{x \in R \mid xr = rx \text{ for all } r \in R\}$$

is called centre of the ring.

One can easily show that Z(R) is a subring of R.

Problem 4 : Find centre of the quaternion ring D.

Solution : Let a = bi + cj + dk ∈ Z(D) be any element. Then it commutes with all elements of D. Thus

(a + bi + cj + dk)(0 + 1i + 0j + 0k) = (0 + 1i + 0j + 0k)(a + bi + cj + dk)

⇒ –b + ai + dj – ck = –b + ai – dj + ck

or 0 + 0i + di – ck = 0 + 0i – dj + ck

or c = 0 and d = 0

Therefore, a + bi + cj + dk = a + bi + 0j + 0k

Now $(a + bi + 0j + 0k)(0 + 0i + 1j + 0k) = (0 + 0i + 1j + 0k)(a + bi + 0j + 0k)$

$\Rightarrow 0 + 0i + aj + bk = 0 + 0i + aj - bk$

Which gives $b = -b$ i.e., $b = 0$

Thus $a + bi + cj + dk = a + 0i + 0j + 0k$

Which shows that $Z(D) \subseteq \{a + 0i + 0j + 0k \mid a \text{ is real number}\}$

Also $a + 0i + 0j + 0k$ commutes with every element of D as a is a real number.

Hence $Z(D) = \{a + 0i + 0j + 0k \mid a \text{ is real number}\}$

or that $Z(D) = \{(a, 0, 0, 0) \mid a \in R\}$

Problem 5 : If R is a division ring then show that the centre Z(R) of R is a field.

Solution : Z(R) is a ring (as it is a subring).

Z(R) is commutative by its definition.

Z(R) has unity as $1. x = x. 1 = x$ for all $x \in R$.

Thus we need to show that every non zero element Z(R) has multiplicative inverse (in Z(R)).

Let $x \in Z(R)$ be any non zero element

Then $x \in R$ and since R is a division ring, $x^{-1} \in R$

Let $y \in R$ be any non zero element, then $y^{-1} \in R$. Now

$$x^{-1} y = (y^{-1} x)^{-1}$$

$$= (xy^{-1})^{-1} = yx^{-1}$$

$\Rightarrow x^{-1}$ commutes with all non zero elements of R.

Again as $x^{-1}. 0 = 0 . x^{-1} = 0$

we find $x^{-1}, r = r. x^{-1}$ for all $r \in R$

$\Rightarrow x^{-1} \in Z(R)$

Showing that Z(R) is a field.

VI. Characteristic of a Ring

Definition : Let R be a ring. If there exists a positive integer n such that $na = 0$ for all $a \in R$ then R is said to have finite characteristic and also the smallest such positive integer is called the characteristic of R.

Thus it is the smallest positive integer n such that $\underset{n\,\text{times}}{1+1+\ldots\ldots+1} = 0$ in R.

If no such positive integer exists then R is said to have characteristic zero (or infinity). Characteristic of R is denoted by char R or ch R.

For Example : (a) Rings of integers, even integers, rationals, reals, complex numbers are all of ch zero.

(b) Consider $R = \{0, 1\}$ mod 2

then ch R = 2 as

$2 \cdot 1 = 1 \oplus 1 = 0$

$2 \cdot 0 = 0 \oplus 0 = 0$

Thus 2 is the least +ve integer s.t., $2a = 0$ for all $a \in R$.

Note $1 \cdot 1 = 1 \neq 0$

(c) If R is a (non zero) finite ring, then ch $R \neq 0$. Let $o(R) = m > 1$. Since $\langle R, + \rangle$ is a group, $ma = 0 \ \forall \ a \in R$. Hence ch $R \neq 0$

Notice ch R = 1 if $R = \{0\}$.

(d) ch $Z_n = n$

By (c) ch $Z_n \neq 0$. Let ch $Z_n = m$

Then $ma = 0 \ \forall \ a \in Z_n$

i.e, $m. 1 = 0$

i.e., $1 \oplus 1 \oplus \ldots\ldots \underset{(m \text{ times})}{\oplus} 1 = 0$

or that $m = nq \Rightarrow n \mid m \Rightarrow m \geq n$

But $na = 0 \ \forall \ a \in Z_n$ as $o(Z_n) = n$

and thus ch $Z_n \leq n$.

i.e., $m \leq n$ giving $m = n$.

Theorem 6 : Let R be a ring with unity. If 1 if of additive order n then ch R = n. If 1 is of additive order infinity then ch R is 0.

Proof : Let additive order of 1 be n. (By this, we mean, order of 1 in the group (R, +) is n). Then $n \cdot 1 = 0$ and n is such least +ve integer.

Now for any $x \in R$

$nx = x + x + \ldots. + x = 1. x + 1. x + \ldots. + 1 \cdot x$

$= (1 + 1 + \ldots\ldots + 1)x = 0 \ x = 0$

Showing that ch R = n.

It 1 has infinite order under addition then $\exists$ no. n s.t., $n. 1 = 0$ and thus

ch R = 0.

Remark : The above result can also be stated as

If R is ring with unity then R has ch $n > 0$ iff n is the smallest positive integer s.t., $n. 1 = 0$

Theorem 7 : If D is an integral domain, then characteristic of D is either zero or a prime number.

Proof : If ch D is zero, we have nothing to prove. suppose D has finite characteric, then $\exists$ a +ve integer m, s.t., $ma = 0$ for all $a \in D$.

Let k be such least +ve integer then ch D = mk. We show k is a prime.

Suppose k is not a prime, then we can write

$k = rs, \ 1 < r, s < k$

Now $ka = 0$ for all $a \in D$

$\Rightarrow (rs)a^2 = 0 \ \forall \ a \in D$

$\Rightarrow a^2 + a^2 + \ldots\ldots + a^2 = 0$ (rs times)

$\Rightarrow \underbrace{(a + a + \ldots\ldots + a)}_{r \text{ times}}\underbrace{(a + a + \ldots\ldots + a)}_{s \text{ timess}} = 0$

$\Rightarrow (ra)\,(sa) = a \ \forall \ a \in D$

$\Rightarrow ra = 0$ or $sa = 0 \ \forall \ a \in D$ (See next problem)

In either case it will be a contradiction as r, s < k, and k is the least +ve integer s.t., ka = 0.

Hence k is a prime.

Problem 6 : If D is an integral domain and if na = 0 for some $0 \neq a \in D$ and some integer $n \neq 0$ then show that the characteristics of D is finite.

Solution : Since na = 0

$(na)x = 0$ for all $x \in D$

$\Rightarrow (a + a + \ldots.+a)\ x = 0$

$\Rightarrow ax + ax + \ldots\ldots + ax = 0$ (n times)

$\Rightarrow a(x + x + \ldots\ldots + x) = 0$ for all $x \in D$

$\Rightarrow x + x + \ldots\ldots + x = 0$ for all $x \in D$ as $a \neq 0$

$\Rightarrow nx = 0$ for all $x \in D$, $n \neq 0$

$\Rightarrow$ ch D is finite.

VII. Idempotent and Nilpotent elements.

Definitions : An element e in a ring R is called idempotent if $e^2 = e$.

An element $a \in R$ is called nilpotent if $a^n = 0$ for some integer n.

If R is a ring with unity, then 0 and 1 are idempotent elements. Alos 0 is nilpotent element of R.

Problem 7 : A non zero idempotent cannot be nilpotent.

Solution : Let x be non zero idempotent, then $x^2 = x$.

If x is also nilpotent then $\exists$ integer $n \geq 1$ s.t.,

$x^n = 0$

But $x^2 = x \Rightarrow x^3 = x^2 = x$

$\Rightarrow x^4 = x^2 = x$

$\Rightarrow x^n = x \Rightarrow x = 0$ a contradiction.

Problem 8 : In an integral domain R (with unity) the only idempotents are the zero and unity.

Solution : Let $x \in R$ be any indempotent

Then $x^2 = x \Rightarrow x^2 - x = 0$

$\Rightarrow x(x - 1) = 0$

$\Rightarrow x = 0$ or $x = 1$ as R is an integral domain.

Remark : A field which is a Boolean ring has only two elements.

Problem 9 : If R is a ring with no non zero nilpotent elements then show that for any idempotent e, ex = xe for all $x \in R$ and thus $e \in Z(R)$.

Solution : e idempotent $\Rightarrow e^2 = e$

Let $x \in R$ be any element, then

$(exe - ex)^2 = exeexe - exeex - exexe + exex$

$= 0$ (using $e^2 = e$)

$\Rightarrow exe - ex$ is nilpotent.

By given condition, $exe - ex = 0 \Rightarrow exe = ex$

Similarly, we get $exe = xe$

Hence $ex = xe$.

VIII. Product of Rings

Let R_1 and R_2 be two rings.

Let $R = \{(a, b) | a \in R_1, b \in R_2\}$, then it is easy to verify that R forms a ring under addition and multiplication defined by

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

$$(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2)$$

i.e., under the usual compositions of component wise addition nd multiplication. This ring is called the direct product of R_1 and R_2. One can similarly extend the definition to product of more than two rings. R_1 and R_2 are called the component rings of the direct product.

IX. Self Check Exercise

1. Show that a ring R is commutative iff

$(a + b)^2 = a^2 + b^2 + 2ab$ for all $a, b \in R$.

2. Let R be a commutative ring with unity. Show that

(i) a is a unit iff a^{-1} is a unit.

(ii) a, b are units iff ab is a unit.

3. Give an example of a non commutative ring R in which $(xy)^2 = x^2y^2$ for all $x, y \in R$.

4. Show that a finite commutative ring R without zero divisors has unity .

5. Show that intersection of two subrings (subfields) is a subring (subfield).

6. Give an example to show that union of two subrings may not be a subring. Prove that union of two subrings is a subring iff one of them is contained in the other.

7. Prove that centre of a ring is a subring.

8. Show that a field of characteristic zero is infinite.

9. If S be a subring of a division ring R, show that ab = 0 in $S \Rightarrow$ either a = 0 or b = 0.

10. In a ring without unity, show that every indempotent is a zero divisor but nor nilpoten.

RINGS – II

Objectives

I. Ideals
II. Sum of Two Ideals
III. Product of Two Ideals
IV. Simple Ring
V. Self Check Exereice.

I. Ideals

Definition : A non empty subset I of a ring R is called a right ideal of R is

(i) $a, b \in I \Rightarrow a - b \in I$

(ii) $a \in I, r \in r \Rightarrow ar \in I$

I is called a left ideal of R if

(i) $a, b \in I \Rightarrow a - b \in I$

(ii) $a \in I, r \in R \Rightarrow ra \in I$.

I is called a two side or both side ideal of R, if it is both left and a right ideal.
In fact, if we say I is an ideal of R, it would mean, I is two sided ideal of R.

Example 1 : In a ring R, {0} and R are always both sided ideals.
Any ideal except these two is called a proper ideal or non trivial ideal.

Example 2 : Let < Z, + , . > be the ring of integers. Then
E = set of even integers is an ideal of Z

$a, b \in E \Rightarrow a = 2n, b = 2m$

Thus $a - b = 2(n - m) \in E$
Again, if $2n \in E, r \in Z$ then as
(2n)r or r(2n) are both in E, E is an ideal.

Example 3 : Let R = ring of 2 × 2 matrices over integers.

Let $A = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \mid a, b \text{ integers} \right\}$

Then A is right ideal of R as

$$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a-c & b-d \\ 0 & 0 \end{bmatrix} \in A$$

$$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}\begin{bmatrix} x & y \\ z & u \end{bmatrix} = \begin{bmatrix} ax+bz & ay+ba \\ 0 & 0 \end{bmatrix} \in A$$

But A is not a left ideal of R as

$$\begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix} \in I, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \in R$$

But $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix} \notin A$

Example 4 : In the same ring as above, one can check that $B = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \mid a, b \text{ integers} \right\}$ forms a left (but not right) ideal of R.

Remark : An ideal is always a subring. Let I be an ideal of a ring R. To show that I is a subring we need to show that for a, b $\in$ I, ab $\in$ I.

Now a, b $\in$ 1 $\Rightarrow$ a $\in$ I, b $\in$ I $\subseteq$ R

$\Rightarrow$ ab $\in$ I (def. of ideal)

Hence I is a subring.

But a subring may not be an ideal.

We know that < Z, +, . > is a subring of < Q, +, $\square$> where Z = integers, Q = rationals.

Now, $3 \in Z, \frac{1}{5} \in Q$. But $3.\frac{1}{5} \notin Z$

Thus Z is not an ideal.

We have talked about intersection and union of subgroups, subrings etc. Similar results hold in case of ideals.

What can we say about intersection of a left and a right ideal? Will it be an ideal? The answer is given by the following example:

If we consider the ideals in example 3, 4, we find A $\cap$ B will have members of the type $\left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \mid a, \text{an integer} \right\}$.

Since $\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}\begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix}=\begin{bmatrix}1 & 1\\ 0 & 0\end{bmatrix}\notin A\cap B$

We notic $A \cap B$ is not a right ideal.

Problem 1 : Let S be a non empty subset of a ring R. Show that $r(s) = \{x \in R \mid Sx = 0\}$ and $I(s) = \{x \in R \mid xS = 0\}$ are rspectively right and left ideals of R.

Solution : $r(x) \neq \varphi$ as $0 \in r(s)$

Again, $x, y \in r(s) \Rightarrow sx = 0, sy = 0$

Now $S(x - y) = Sx - Sy = 0 - 0 = 0$

$\Rightarrow x - y \in r(s)$

Again, if $r \in R$ be any element then

$S(xr) = (Sx)r = 0, r = 0$

$\Rightarrow xr \in r(s)$

Hence r(s) is a right ideal. Similarly, l(s) will form a left ideal.

r(s) and l(s) are called right and left annihilators of S, respectively.

Both r(s) and l(s) will be ideals of R if S in an ideal. (Verify!)

Problem 2 : Let R be a ring such that every subring of R is an ideal of R. Further, $ab = 0$ in $R \Rightarrow a = 0$ or $b = 0$. Show that R is commutative.

Solution : Let $0 \neq a \in R$ be any element.

Then $N(a) = \{x \in R. \mid xa = ax\}$ is a subring of R and, therefore, an ideal of R.

Let $r \in R$ be any element. Since $a \in N(a)$, $r \in R$ we find $ra \in N(a)$ (Def. of ideal)

Also then, $a(ra) = (ra)a$

and so $(ar - ra)\, a = 0$

$\Rightarrow$ $ar - ar = 0$ as $a \neq 0$

Thus $ar = ra \ \forall\ r \in R, \forall\ 0 \neq a \in R$

and as $0.r = r.0 = 0$ we find

$ar = ra \ \forall\ a, r \in R$

Hence R is commutative.

II. Sum of Two Ideals

Let A and B be two ideals of a ring R. We define A + B to be the set $\{a + b \mid a \in A, b \in B\}$, called sum of the ideals A and B.

Theorem 1 : If A and B are two ideals of R then A + B is an ideal of R, containing both A and B.

Proof : $A + B \neq \varphi$ as $0 = 0 \in A + B$

Again, $x, y \in A + B$

$\Rightarrow x = a_1 + b_1$

$y = a_2 + b_2$ for some $a_1, a_2 \in A$; $b_1, b_2 \in B$

Since $x - y = (a_1 + b_1) - (a_2 + b_2)$

$= (a_1 - a_2) + (b_1 - b_2)$

we find $x - y \in A + B$

Let $x = a + b \in A + B$, $r \in R$ be any elements then

$xr = (a + b)r = ar + br \in A + B$ as A, B are ideals

$rs = r(a + b) = ra + rb \in A + B$

Thus A + B is an ideal of R.

Again for any $a \in A$, since $a = a + 0 \in A + B$ and for any $b \in B$, since $b = 0 + b \in A + B$

We find $A \subseteq A + B$

$B \subseteq A + B$

Remarks : (i) We can show that A is an ideal of A + B

$a_1, a_2 \in A \Rightarrow a_1 - a_2 \in A$ is an ideal of R. Again, if $a \in A$ and $s \in A + B$ be any elements then $s = a_1 + b_1$ for some $a_1 \in A$, $b_1 \in B$

also $as = a(a_1 + b_1)$

$= aa_1 + ab_1 \in A$

as $a, a_1 \in A \Rightarrow aa_1 \in A$

$a \in A, b_1 \in B \subseteq R \Rightarrow ab_1 \in A$

$\Rightarrow aa_1 + ab_1 \in A$

Similarly, $sa \in A$. Showing that A is an ideal of A + B.

(ii) If A is a left ideal and B, a right ideal of R then A + B may not be an ideal of R. Considering the same ideals as in examples 3, 4, we find

A + B will have members of the type $\begin{bmatrix} a & b \\ c & 0 \end{bmatrix}$

and as $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix} = \begin{bmatrix} 4 & 4 \\ 2 & 2 \end{bmatrix} \notin A + B$

A + B is not an ideal of R.

Definition : Let S be any subset of a ring R. An ideal A of R is said to be generated by S if

(i) $S \subseteq A$

(ii) for any ideal I of R, $S \subseteq I \Rightarrow A \subseteq I$.

We denote if by writing A = <S > or A = (S)

In fact < S > will be intersection of all ideals of R that contain S, and is the smallest ideal containing S. If S is finite, we say A = < S > is finitely generated.

If S = φ then as {0} is an ideal of R containing S = φ, $< S > \subseteq \{0\}$ and so $< S > = \{0\}$
If S = {a} then we denote < S> by < a > or (a). By definition, $a \in < a >$ and as it is an ideal, elements of the type ra, as, r_1 as_1, na are in < a >, where r, r_1, s, $s_1 \in R$ and n is an integer. Such an ideal is called a principal ideal generated by a.

Theorem 2 : If A and B be two ideals of a ring R. then

$A + B = < A \cap B$.

Proof : We have already proved that A + B is an ideal of R, containing A and B, thus A + B is an ideal containing $A \cup B$.

Let I be any ideal of R, s.t., $A \cup B \subseteq I$
Let $x \in A + B$ be any element
Then $x = a + b$ for some $a \in A, b \in B$
Since $a \in A \subseteq A \cup B \subseteq I$
$a \in B \subseteq A \cup B \subseteq I$
we find $a = b \in I$ as I is an ideal
$\Rightarrow x \in I$ or that $A + B \subseteq I$
which proves the theorem.

Thus A + B is the smallest ideal of R, containing A and B. One can, of course, talk about sum of more than two ideals in the same manner.

Problem 3 : If $a \in R$ be an element and $I = aR = \{ar \mid r \in R\}$ where R is a commutative ring, then I is as ideal of R.

Solution : $I \neq \varphi$ as $0 = a.\ 0 \in I$

$x, y \in I \Rightarrow x = ar_1$, $y = ar_2$ for some $r_1, r_2 \in R$
$\Rightarrow x - y = a(r_1 - r_2) \in I$
again if $x = ar_1 \in I$ and $r \in R$ be any elements

then $x\ r = (ar_1)r = a(r_1\ r) \in I$ shows that I is a right ideal. R being commutative, it will be both sided ideal.

Remark : If the ring is not commutative, one can show that aR is a right ideal and $Ra = \{ra \mid r \in R\}$ is a left ideal of R.
aR is always contained in < a >. If R is a commutative ring with unity then aR = Ra = (a).
Now, we understand the difference between aR and < a > through the following example.

Example : Let < E, +, > be the ring of even integers. It is commutative ring without unity. Let $a = 4 \in E$
Then $< 4 > = \{4n + (2m)\ 4 \mid n, m \in Z\}$
$= \{4n + 8m \mid n, m \in Z\}$
Whereas $4E = \{4(2k) \mid k \in Z\} = \{8k \mid k \in Z\}$

We notice then, $< 4 > \neq 4E$ as $4 \in < 4 >$ but $4 \notin 4E$.

Problem 4 : If A is an ideal of a ring R with unity such that $1 \in A$ then show that A = R.

Solution : Since $A \subseteq R$ always, all we need to show is that $R \subseteq A$.

Let $r \in R$ be any element.

Since $1 \in A$ and A is an ideal.

$r = 1.\ r \in A$

$\Rightarrow R \subseteq A$ or that A = R.

Problem 5 : Determine all the ideals of the ring of integers $< Z, +, . >$.

Solution : Let I be any ideal of $< Z, +, . >$ then as $a, b \in I \Rightarrow a - b \in I$, we notice $<I, + >$ is a subgroup of $< Z, + >$

Since $< Z, + >$ is a cyclic group generated by 1, I will be a cyclic group generated by a multiple of 1, say n.

Thus any ideal of $< Z, + . >$ is of the type $< n >$, ie., multiple of some integer. Conversely it is easy to see that $< n >$ for any integer n is an ideal.

III. Product of Two Ideals

Let A, B be two ideals of a ring R. We define the product AB of A and B by

$AB = \{\Sigma\ a_i b_i \mid a_i \in A,\ b_i \in B\}$

where summation is finite.

Theorem 3 : The product AB of any two ideals A and B of a ring R is an ideal of R.

Proof : $AB \neq \varphi$ as $0 = 0.\ 0 \in AB$

Let $x, y \in AB$ be any two members

then $x = a_1b_1 + a_2b_2 + \ldots\ldots + a_nb_n$

$y = a_1'b_1' + \ldots\ldots + a_m'b_m'$

for some $a_i, a_j' \in a, b_i, b_j' \in B$

$$x - y = (a_1b_1 + \ldots\ldots + a_nb_n) - \left(a_1'b_1' + \ldots\ldots + a_m'b_m'\right)$$

Which clearly belongs to AB, as the R.H.S. can be written as

$x_1y_1 + x_2y_2 + \ldots\ldots\ldots + x_ky_k$ $\qquad (k = n + m)$

where $x_i \in A,\ y_i \in B$

Again, for any $x = a_1b_1 + \ldots\ldots\ldots + a_nb_n \in AB$ and $r \in R$.

$rx = r(a_1b_1 + \ldots\ldots\ldots + a_nb_n)$

$= (ra_1)b_1 + (ra_2)b_2 + \ldots\ldots + (ra_n)b_n \in AB$

because $ra_i \in A$ as $a_i \in A$,$r \in R$, and A is an ideal.

Similarly $xr \in AB$

showing thereby that AB is an ideal of R.

IV. Simple Ring

Definition : A ring $R \neq \{0\}$ is called a simple ring if R has no ideals except R and {0}.

Theorem 4 : A division ring is a simple ring.

Proof : Let R be a division ring. Let A be any ideal of R s.t., $A \in \{0\}$ then $\exists$ at least one $a \in A$ s.t., $a \neq 0$. R being a division ring, $a^{-1} \in R$ and $aa^{-1} = 1$.

Since $a \in A$, $a^{-1} \in R$, $aa^{-1} \in A$ (def. of ideal)

$\Rightarrow 1 \in A$

$\Rightarrow A = R$

i.e., only ideals that R can have are R and {0} or that R is a simple ring.

Problem 6 : Let R be a ring with unity, such that R has no right ideals except {0} and R. Show that R is a division ring.

Solution : To prove : Non zero elements of R form a group under multiplication.

Let $0 \neq a \in R$ be any non zero element.

Let $aR = \{ar \mid r \in R\}$

Then aR is a right ideal.

By given condition, then

$aR = R$

or $aR = \{0\}$

But $aR \neq \{0\}$ as $a \neq 0$ and $a = a.1 \in aR$

Hence $aR = R$

Now $1 \in R \Rightarrow 1 \in aR \Rightarrow \exists\ b \in R$, s.t. $1 = ab \Rightarrow$ b is right inverse of a (w.r.t multiplication). Thus $< R - \{0\}. >$ forms a group or that R is a division ring.

Problem 7 : Let R be a ring having more than one element such that aR = R, for all $o \neq a \in R$. Show that R is a division ring.

Solution : We first show that $xy = 0 \Rightarrow x = 0$ or $y = 0$ in R.

So let $xy = 0$ and suppose $x \neq 0$, $y \neq 0$

Then $xR = yR = R$

Also $(xy)R = x(yR) = xR = R$

$\Rightarrow R = \{0\}$ as $xy = 0$

contradicting that R has more than one element.

Hence our assertion is proved

Again, as $R \neq \{0\}$, $\exists\ 0 \neq a \in R$ and by given condition then $aR = R$

$\Rightarrow \exists\ e \in R$ s.t., $ae = a$ $\quad (e \neq 0$ as $a \neq 0)$

$\Rightarrow ae^2 = ae$

$\Rightarrow a(e^2 - e) = 0$

$\Rightarrow e^2 = e$ as $a \neq 0$

We claim e is right unity of R.

If e is not right unity of R, then $\exists\ y \in R$ s.t., $ye \neq y$

But $(ye - y)e = ye^2 - ye = ye - ye = 0$

$\Rightarrow$ either $ye = y$ or $e = 0$, a contradiction

$\Rightarrow$ e is right unity of R.

Let $0 \neq a \in R$ be any element then $aR = R$

Now $e \in R$, $aR = R$,

$\Rightarrow e \in aR \Rightarrow \exists\ b \in R$, s.t., $e = ab$

or that b is right inverse of a.

$\Rightarrow$ every non zero element of R has right inverse.

Hence R is a division ring.

V. Self Check Exereice :

1. Show that intersection of two ideals in an ideal.

2. Give an example to show that union of two ideals may not be an ideal.

3. Prove that union of two ideals is an ideal iff one of them is contained in the other.

4. Let R be the ring of 2 × 2 matrices over integers, If $a = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \in R$, then show that aR is not a left ideal of R.

5. Let R be a non commutative ring with unity. Show that Z(R), the centre of R is not an ideal of R. [Hint : Z(R) is properly contained in R].

6. If F is a field, prove that its only ideals are {0} and F.

7. Show that if an ideal A of a ring R with unity contains a unit of R then A = R.

8. Let A, B be two subrings of a ring R such that for all $a \in A$, $b \in B$, ab, $ba \in A$ then show that

(i) A + B is a subring of R.

(ii) A is an ideal of A + B.

(iii) $A \cap B$ is an ideal of B.

LESSON NO. 2.3 **AUTHOR : DR. CHANCHAL**

RINGS – III

Objectives

I. Quotient Rings
II. Ring Homomorphisms
III. Kernel of a Ring Homomorphirm
IV. Fundamental Theorem of Ring Homomorphism
V. First Theorem of Isomorphism
VI. Second Theorem of Isomorphism
VII. Embedding of Rings
VIII. Self Check Exercise

I. Quotient Rings

Let R be a ring and let I be an ideal of R. Since a, b $\in$ 1 $\Rightarrow$ a – b $\in$ I, So I is a subgroup of < R, + >. Again as < R, + > is abelian, I will be a normal subgroup of R and we can talk of $\frac{R}{I}$, the quotient group

$\frac{R}{I} = \{r + 1 \mid r \in R\}$ = set of all cosets of I in R (clearly left or right cosets are equal)

We know R/I forms a group under 'addition' defined by

$(r + I) + (s + I) = (r + s) + 1$

We now define a binary composition (product) on R/I by

$(r + I)(s + I) = rs + 1$

We show this product is well defined

Let $r + I = r' + 1$ and $S + I = s' + I$,

$\Rightarrow r - r' \in I \text{ and } s - s' \in I$

$\Rightarrow r - r' = a \text{ and } s - s' = b \text{ for some } a, b \in I$

$\Rightarrow r = r' + a, s = s' + b$

$\Rightarrow rs = (a + r')(b + s')$

$$\Rightarrow rs + I = (ab + as' + r'b + r's') + I = r's' + I$$

(using $x + I = I$ iff $x \in I$)

Hence the multiplication is well defined.

Since $(a + I)[(b + I)(c + I)] = (a + I)(bc + I)$

$$= a(bc) + I$$

$$= (ab)c + I$$

$$= (ab + I)(c + I)$$

$$= [(a + I)(b + I)](c + I)$$

Associativity holds w.r.t this product.

Again, as $(a + I)[(b + I) + (c + I)] = (a + I)(b + c + I)$

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

$$= (ab + ac) + I$$

$$= (ab + I) + (ac + I)$$

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

We find left distributivity holds. Similarly one can check that right distributivity also holds in R/I and hence R/I forms a ring, called the quotient ring or factor ring or residue class ring of R by I.

We look at it from another angle. Let R be a ring and I an ideal of R. Define, for $a, b \in R, a \equiv b \pmod{I}$ if $a - b \in I$. It is easy to check that this relation is an equivalence relation on R. Thus it partitions R into equivalence classes. Let for any $a \in R, cl(a)$ be the corresponding equivalence class of a.

Then $cl(a) = \{r + R \mid r = a \pmod{I}\}$

$$= \{r \in R \mid r - a \in I)\}$$

$$= \{r \in R \mid r - a = x \text{ for some } x \in I)\}$$

$$= \{r \in R \mid r = a + x \text{ for some } x \in I)\}$$

$$= \{a + x \mid x \in I\}$$

$= a + 1$

Thus, the quotient ring $\frac{R}{I}$ is nothing but the ring of all equivalence classes as defined above.

In fact, the binary compositions defined can be stated as:

$$cl(a) + cl(b) = cl(a + b) \qquad a, b \in R$$

$$cl(a).cl(b) = cl(ab)$$

One can verify that R/I froms a ring. In fact, if R has unity 1 then cl(1) will be unity of R/I.

R/I is therefore also called quotient ring of R modulo I.

Remarks : (i) It may be noticed that R/I is defined only when I is an ideal of R. If is only a subring of R, then R/I may not form a ring as the multiplication rule may not be valid. Suppose I is only a subring of R (and is not an ideal), let $r \in R, a \in I$ s.t., $ar \notin I$

Then $(a + I)(r + I) = ar + I$

gives $(0 + I)(r + I) = ar + I$ as $a \in I \Leftrightarrow a + I = I = 0 + I$

i.e, $0.r + I = ar + I$ or that $ar \in I$ which is not true.

(ii) If I = R then R/I is isomorphic to the zero ring {0} and if I = {0} there $\frac{R}{I} \cong R$.

Example : Let $H_4 = \{4n \mid n \in Z\}$, where < Z, +, .> is the ring of integers. Then H_4 is are ideal of Z and thus $\frac{Z}{H_4}$ is a quotient ring and is given by

$$\frac{Z}{H_4} = \{H_4, H_4 + 1, H_4 + 2, H_4 + 3\}$$

This example also shows us that quotient ring of an integral domain may not be an integral domain.

Notice $(H_4 + 2)(H_4 + 2) = H_4 + 4 = H_4 = \text{zero of } \frac{Z}{H_4}$ but $H_4 + 2 \neq H_4$

On the other hand if we cosider

$R = \{0, 2, 4, 8, 10\} \bmod 12$

$S = \{0, 6\} \bmod 12$

then R is not an integral domain whereas R/S is an integral domain.

We have $R/S = \{S, S+2, S+4\}$

Since $(S+2)(S+2) = S+2, (S+2)(S+4) = S+8 = S+2$

and $(S+4)(S+4) = (S+16) = S+4,$ we find

$\frac{R}{S}$ has no zero divisors.

II. Ring Homomorphisms

Let <R, +, □ >, < R', *, 0> be two rings. A mapping $\theta : R \to R'$ is called a homomorphism ir

$$\theta(a+b) = \theta(a) * \theta(b)$$

$$\theta(ab) = \theta(a) o \theta(b) \qquad a, b \in R$$

Since we prefer to use the symbols + and □ for the binary compositions in a ring, the above definition can be simplified by saying that a mapping $\theta = R \to R'$ is called a homomorphism if

$$\theta(a+b) = \theta(a) + (b)$$

$$\theta(ab) = \theta(a).(b)$$

Similarly, we can talk about isomorphism in rings as a one-one onto homomorphism.

Example : Consider the map $f : C \to C$, s.t.,

$$f(a+ib) = a - ib$$

then f is a homomorphism, where C = complex numbers,

as $f\left[(a+ib)+(c+id)\right] = f\left((a+c)+i(b+d)\right)$

$$= (a+c) - i(b+d)$$

$$= (a-ib) + (c-id)$$

$$= f(a+ib) + f(c+id)$$

and $f\left[(a+ib)(c+id)\right] = f\left((ac-bd)+i(ad+bc)\right)$

$= (ac-bd)-i(ad+bc)$

$= (a-ib)c-id(a-ib)$

$= (a-ib)(c-id)$

$= f(a+ib)f(c+id)$

Theorem 1: If $\theta : R \to R'$ be a homomorphism, then (i) $\theta(0) = 0'$, (ii) $\theta(-a) = -\theta(a)$; where O,O' are zeros of the rings R, R' respectively.

Proof : (i) Since 0 + 0 = 0

we have $\theta(0+0) = \theta(0)$

$\Rightarrow \theta(0)+\theta(0) = \theta(0)+0'$

$\Rightarrow \theta(0) = 0'$

(ii) Again, as a + (–a) = 0

$\theta(a+(-a)) = \theta(0)$

$\Rightarrow \theta(a)+\theta(-a) = \theta(0) = 0$

$\Rightarrow -\theta(a) = \theta(-a)$

Cor.: It is clear that

$\theta(a-b) = \theta(a+(-b))$

$= \theta(a)-\theta(b)$

Remark : The terminolgy of epimorphism, monomorphism etc, is extended to rings also in the same way as in groups.

III. Kernel of a Ring Homomorphirm

Definition : Let $f : R \to R'$ be a homomorphism, we define Kernel of f by

$$\text{Ker } f = \{x \in R \mid f(x) = 0'\}$$

where 0' is zero of R'.

The following two theorems are easy to prove and left as an exercise for the reader.

If $f : R \to R'$ is a homomorphism then

Theorem 2 : Ker f is an ideal of R.

Theorem 3 : Ker f = (0) iff f is one-one.

Problem 1 : If R is ring with unity and f : R $\to$ R' is a homomorphism where R' is an integral domain such that Ker f $\neq$ R thens show that f(1) is unity of R'.

Solution : Let a' $\in$ R' be any element. We show

$$f(1)\ a' = a'f(1) = a'$$

Now $f(1)\ a' - f(1)\ a' = 0'$

$\Rightarrow f(1.1)\ a' - f(1)\ a' = 0'$

$\Rightarrow f(1)\ f(1)\ a' - f(1)\ a' = '$

$\Rightarrow f(1)\ [f(1)\ a' - a'] = 0'$

$\Rightarrow$ eiter $f(1) = 0'$ or $f(1)\ a' - a' = 0'$ as R' is an integral domain.

$f(1) = 0' \Rightarrow 1 \in \text{Ker } f \Rightarrow \text{Ker } f = R$ which is not true.

Hence $f(1)\ a' - a' = 0'$

$\Rightarrow$ $f(1)\ a' = a'$

Similarly, we can show $a' = a'f(1)$.

Problem 2 : Let f : R $\to$ R' be an onto homomorphism, where R is a ring with unity. Show that f(1) is unity of R'.

Solution : Let a' $\in$ R' be any element.

Since f is onto, $\exists$ a $\in$ R, s.t., f(a) = a'

Now $a'.\ f(1) = f(a).\ f(1) = f(a.\ 1) = f(a) = a'$

Similarly f(1), a' = a'.

Showing, thereby that f(1) is unity of R'.

Problem 3 : Show by an example that we can have a homomorphism $f : R \to R'$, such that f (1) is not unity of R', where 1 is unity of R.

Solution : Consider the map f: Z $\to$ Z', s.t.,

$f(x) = 0$ for all $x \in Z$

where Z = ring of integers

then f is a homomorphism (verify)

Again f(1) = 0, but 0 is not unity of Z.

Thus although Z (on R.H.S.) has unity but the unity is not equal to f(1).

Remarks : (i) If we take the map f : Z $\to$ E, where E = ring of even integers, defined by f (x) = 0 for all x, we find , E does not have unity, whereas 1 is unity of Z.

(ii) The map f : Z $\to$ E, s.t., f(x) = 2x is a group isomorphism. Thus Z and E are isomorphic as groups whereas Z and E are not isomorphic as rings. Indeed, Z has unity but E does not possess unity. In fact, f will not be a ring homomorphism.

Problem 4 : Show that 2Z is not isomorphic to 3Z as rings. What can be said about isomorphism between mZ and nZ, where m, n are positive integers?

Solution : Suppose $2Z \cong 3Z$ and let f : $2Z \to 3Z$ be the isomorphism.

As $2 \in 2Z, f(2) = 3n$ for some $n \in Z$

Now $f(4) = f(2 + 2) = f(2) + f(2) = 6n$

$f(4) = f(2.2) = f(2).f(2) = (3n)^2$

Thus $6n = 3n^2$ or that $2 = 3n$

But this is not possible for any $n \in Z$

Hence f is not an isomorphism.

Suppse now f : $mZ \to nZ$ is any ring isomorphism

Then $$\underset{m\,\text{times}}{f(m + m + ... + m)} = f(m) + f(m) + ... + f(m)$$

$$= mf(m)$$

$$\Rightarrow f(mm) = mf(m)$$

$$\Rightarrow f(m)f(m) = mf(m) \Rightarrow f(m) = m \qquad \ldots (1)$$

Again as f is onto and $n \in nZ, \exists mr \in mZ$

s.t., $f(mr) = n$ or $f(m)f(r) = n$

$$\Rightarrow f(m) \mid n$$

Again as $m \in mZ, f(m) \in nZ$

$$\Rightarrow f(m) = nk \text{ for some } k$$

$$\Rightarrow n \mid f(m)$$

and hence $f(m) = n$

or that $m = n$ from (1)

so if $mZ = nZ$, then $m = n$. The converse is obviously true.

Hence we conclude : $mZ \cong nZ$ as rings if and only if $m = n$.

Problem 5 : Let Z be the ring of integers. Show that the only homomorphisms from $Z \to Z$ are the identity and zero mappings.

Solution : Let f ; $Z \to Z$ be a homomorphism

Since $(f(1))^2 = f(1)\ f(1) = f(1.1) = f(1)$

$f(1)\ [f(1) - 1] = 0$

$$\Rightarrow f(1) = 0 \text{ or } f(1) = 1$$

If $f(1) = 0$ then $f(x) = 0 \forall$ integers x

as $f(x) = f(1.x) = f(1)f(x) = 0.f(x) = 0 \forall x$

Thus in this case f is the zero homomorphism.

if $f(1) = 1$, then for any $x \in Z$

$$f(x) = f(1+1+\ldots+1) = xf(1) = x \qquad (x > 0)$$

$$f(x) = f(-y) = -f(y) = -\left[f(1+1+\ldots+1)\right] = -y\,f(1) = x\,f(1) = x$$

$$(x < 0, y = -x)$$

$f(0) = 0$

So in this case f is identity map, which proves the result.

Probelm 6 : Let R and S be two commutative rings with unity and let f: $R \to S$ be an onto homomorphism. If ch $R \neq 0$, show that ch S divides ch R.

Solution : Suppose ch R = n, then n is least +ve integer such that $na = 0 \forall a \in R$

So $nI = 0$ and n is least

$\Rightarrow 1 + 1 + \ldots. + 1 = 0$ and so additive order of 1 is n.

Again as f is onto, f(1) is unity of S and so ch S is additive order of f(1)

As $o(f(1)) \mid o(1)$, we find ch $S \mid$ ch R.

Problem 7 : Show that the ring D of quaternions is isomorphic to the ring

$$M = \left\{ \begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix} \mid a, b \in C \right\}.$$

Solution : Let $a + bi + cj + dk \in D$.

Then $a + bi + cj + dk = (a + bi) + (c + di)\,j$

Define $\theta : D \to M$, s.t.,

$$\theta(a + bi + cj + dk) = \begin{bmatrix} a + bi & c + di \\ -(c - di) & a - bi \end{bmatrix}$$

Then θ is a ring homomorphism.

θ preserves addition verify.

Consider $\theta\left((a + bi + cj + dk)(a' + b'i + c'j + d'k)\right)$

$$= \theta\left[\left((a + bi) + (c + di)\,j\right)\left((a' + b'i) + (c' + d'i)\,j\right)\right]$$

$$= \theta\left[(a + bi)(a' + b'i) + (a + bi)(c' + d'i)\,j\right.$$

$$+(c+di)(a'-b'i)j+(c+di)(-c'+d'i)i\Big]$$

$$=\begin{bmatrix}(a+bi)(a'+b'i)+(c+di)(-c'+d'i) & (a+bi)(c'+di)+(c+di)(a'-b'i)\\(-c+di)(a'+b'i)+(a-bi)(-c'+d'i) & (a-bi)(a'-b'i)+(c+di)(c'+d'i)\end{bmatrix}$$

$$=\begin{bmatrix}a+bi & c+di\\-c+di & a-bi\end{bmatrix}\begin{bmatrix}a'+b'i & c'+d'i\\-c'+d'i & a'-b'i\end{bmatrix}$$

If is not difficult to check that θ is one-one and onto. So, θ is an isomorphism.

Hence $D \cong M$.

IV. Fundamental Theorem of Ring Homomorphism

Theorem 4 : If $f = R \to R'$ be an onto homomorphism, then R' is isomorphic to a quotient ring of R. In fact, $R' \cong \frac{R}{\text{Ker}\, f}$.

Proof : Let $f : R \to R'$ be onto homomorphism

Define $\varphi : \frac{R}{\text{Ker}\, f} \to R'$, s.t.,

$\varphi(x+I) = f(x)$ for all $x \in R$ where $I = \text{Ker } f$

then φ is well defined as

$x + I = y + I$

$\Rightarrow x - y \in I = \text{Ker } f$

$\Rightarrow f(x-y) = 0$

$\Rightarrow f(x) - f(y) = 0$

$\Rightarrow f(x) = f(y)$

$\Rightarrow \varphi(x+I) = \varphi(y+1)$

Retracing the steps backwards we prove φ is 1–1.

Again, as

$$\varphi\Big[(x+I)+(y+I)\Big] = \varphi\big((x+y)+I\big) = f(x+y) = f(x)+f(y)$$

$$= \varphi(x+I)+\varphi(y+I)$$

$$\varphi\Big[(x+I)+(y+I)\Big] = \varphi(xy+I) = f(xy) = f(x)f(y)$$

$$= \varphi(x+I) + \varphi(y+I)$$

$\Rightarrow \varphi$ is a homomorphism.

Now if $r' \in R'$ be any element then as $f : R \to R'$ is onto, $\exists\, r \in R$, s.t., $f(r) = r'$ for this r, as $\varphi(r + I) = f(r) = r'$

We find $r + I$ is required pre-image of r' under φ showing thereby that φ is onto and hence an isomorphism.

Thus $\frac{R}{\text{Ker}\, f} \cong R'$. By symmetry $R' \cong \frac{R}{\text{Ker}\, f}$

V. First Theorem of Isomorphism

Theorem 7 : Let $B \subseteq A$ be two ideals of a ring R. Then

$$\frac{R}{A} \cong \frac{R/B}{A/B}$$

Proof : Define a mapping $f : \frac{R}{B} \to \frac{R}{A}$ s.t.,

$$f(r+B) = r + A$$

then f is an onto homomorphism (Prove!)

By fundamental theorem, $\frac{R}{A} \cong \frac{R/B}{\text{Ker}\, f}$

Again, since $r + B \in \text{Ker}\, f \Leftrightarrow f(r+B) = A$

$$\Leftrightarrow r + A = A$$

$$\Leftrightarrow r \in A$$

$$\Leftrightarrow r + B \in \frac{A}{B}$$

we find Ker f = A | B

Hence $\frac{R}{A} \cong \frac{R \mid B}{A \mid B}$

VI. Second Theorem of Isomorphism

Theorem 8 : Let A, B be two ideals of a ring R, then

$$\frac{A+B}{A} \cong \frac{B}{A \cap B}$$

Proof : Define a mapping $f : B \to \frac{A+B}{A}$ s.t.,

$$f(b) = b + A \text{ for all } b \in B$$

Then f is a well defined homomorphism

Again if $x + A \in \frac{A+B}{A}$ be any element then

$$x \in A + B \Rightarrow x = a + b, a \in A, b \in B$$

So, $x + A = (a + b) + A = (b + a) + A = b + (a + A) = b + A$

thus $x + A = b + A = f(b)$

i.e., b is the pre-image of x + A under f or that f is onto.

By fundamental theorem then $\frac{A+B}{A} \cong \frac{B}{\text{Ker } f}$

Now $x \in \text{Ker } f \Leftrightarrow f(x) = A$

$$\Leftrightarrow x + A = A \Leftrightarrow x \in A$$

$$\Leftrightarrow x \in A \cap B \qquad (x \in \text{Ker } f \subseteq B)$$

Hence Ker f = $A \cap B$

and thus $\frac{A+B}{A} \cong \frac{B}{A \cap B}$

Remark : Clearly then $\frac{A+B}{B} \cong \frac{A}{A \cap B}$

Problem 8 : Show that $\frac{Z}{<2>} \cong \frac{5Z}{10Z}$.

Solution : Take $A = <2>, B = <5> = 5Z$, the ideals of Z.

Then $A + B = <d>$, where d = g.c.d (2, 5) = 1

$$A \cap B = <1>, \text{where } l = l.\text{c.m } (2, 5) = 10$$

So $A + B = <1> = Z$

$$A \cap B = <10> = 10Z$$

Hence using the above result that

$\frac{A+B}{A} \cong \frac{B}{A \cap B}$ we get $\frac{Z}{<2>} \cong \frac{5Z}{10Z}$.

VII. Embedding of Rings

Let R and R' be two rings. A one-one homomorphism θ from R to R' is called an embedding (imbedding) mapping and in that case R' is called extension ring or overring of R.

Embedding of a ring into a ring with unity.

Let R be any ring and let Z be the ring of integers.

Consider $R \times Z = \{(r, n) \mid r \in R, n \in Z\}$

We show R × Z forms a ring with unity, under addition and multiplication defined by

$$(r,n)+(s,m)=(r+s,n+m) \quad r,s \in R, n, m \in Z$$

$$(r,n).(s,m)=(rs+ns+mr, nm)$$

Addition is well-defined as

Let $(r,n)=(r',n')$ and $(s,m)=(s',m')$

Then $r'=r', n=n'$ and $s=s', m=m'$

$$\Rightarrow r+s=r'+s', n+m=n'+m'$$

$$\Rightarrow (r+s,n+m)=(r'+s', n'+m')$$

Similarly one can show that multiplication is well defined.

Associativity : (r, n) + [(s, m) + (t, k)] = (r, n) + (s + t, m + k)

$$=(r+(s+t), n+(m+k))$$

$$=((r+s)+t, (n+m)+k)$$

$$=(r+s, n+m)+(t,k)$$

$$=[(r,n)+(s+m)]+(t,k)$$

Commutativity follows as above.

Again it is clear that (0, 0) will be the zero element and (–r, –n) will be additive inverse of (r, n), where of course, –r is inverse of r in R and –n is –ve of n in Z.

It is easy to check that associativity w.r.t. multiplication and distributive properties also hold.

Again, as (r, n) (0, 1) = (r. 0 + n.0 + 1r, n.1)

= (r, n)

(0, 1) will be unity and hence R × Z forms a ring with unity.

We show R can be imbedded into R × Z

Define a mapping $\theta : R \to R \times Z$, s.t.,

$$\theta(r) = (r, 0)$$

then θ is clearly well defined mapping

Also $\theta(r) = \theta(s)$

$$\Rightarrow (r, 0) = (s, 0) \Rightarrow r = s$$

shows θ is one-one.

Again $\theta(r + s) = (r + s, 0) = (r, 0) + (s, 0) = \theta(r) + \theta(s)$

$$\theta(rs) = (rs, 0) = (r, 0)(s, 0) = \theta(r)\,\theta(s)$$

Thus θ is a homomorphism and therefore, an embedding mapping.

Hence we get

Theorem 9 : Any ring can be embedded into a ring with unity.

Embedding of a ring into a ring of endomorphisms

We recall that a homomorphism from A to A is called an endomorphism.

Let < V, + > be any additive abelian group. We denote by Hom (V, V) the set of all homomorphisms from V to V (i.e. it is set of all endomorphisms of V).

We show now Hom (V, V) forms a ring with unity under the operations defined by

$$(f + g)x = f(x) + g(x) \quad x \in V$$

$$(fg)x = f(g(x)) \quad x \in V$$

where $f, g \in$ Hom (V, V).

Clossure : Let $f, g \in$ Hom (V, V)

Then $(f + g)(x + y) = f(x + y) + g(x + y)$

$$= (f(x) + f(y)) + (g(x) + g(y))$$

$$= (f(x) + g(x)) + (f(y) + g(y))$$

$$= (f + g)x + (f + g)y$$

$\Rightarrow$ f + g is an endomorphism of V

i.e., $f + g \in \text{Hom } (V, V)$

Again $(fg)(x+y) = f\big(g(x+y)\big)$

$= f\big(g(x) + g(y)\big)$

$= f\big(g(x)\big) + f\big(g(y)\big)$

$= (fg)x + (fg)y$

$\Rightarrow fg \in \text{Hom}(V, V)$

Associativity : $\big[f + (g+h)\big]x = f(x) + \big[(g+h)x\big]$

$= f(x) + \big(g(x) + h(x)\big)$

$= \big(f(x) + (g(x)\big) + h(x)$

$= (f+g)x + h(x)$

$= \big[(f+g) + h\big]x$ for all x

$\Rightarrow f + (g+h) = (f+g) + h$

Commutativity follows as above.

Let $O : V \to V$ be defined by

$O(x) = 0$ for all $x \in V$

Then O is easily seen to be a homomorphism.

Also since $(f+O)x = f(x) + O(x) = f(x) + 0 = f(x)$

$= 0 + f(x) = O(x) + f(x) = (O+f)x$ for all x

we have

$f + O = f = O + f$

or that O is zero of Hom (V, V).

Again for any f$\in$ Hom (V, V), define a map

(–f) : $V \to V$, s.t.,

(–f) x = –f (x)

then (–f) is a homomorphism and f + (–f) = O = (–f) + f

Showing thereby that (–f) is inverse of f. Associativity and distributivity can be proved easily, establishing that Hom (V, V) is a ring. The map $i : V \to V$ s.t., $i(x) = x$ for all $x \in V$ will act as unity of this ring.

Hence Hom (V, V) forms a ring with unity for any additive abelian group V.

Theorem 10 : An integral domain can be embedded into a field.

Prof. Try Yourself.

VIII. Self Check Exercise

1. Show that the relation of isomorphism is rings is an equivalence relation.

2. Show that homomorphic image of a commutative ring is commutative. Prove also that the converse may not hold.

3. Let I be an ideal of a ring R. Show that

(a) if R is commutative then so is R/I

(b) If R has unity 1 then 1 + I is unity of R/I

(c) converse of (a) and (b) does not hold.

[Hint : Take R = ring of matrices of the type $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ and I of type $\begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix}$ over integers.]

4. Let $f : R \to R'$ be a homomorphism and let A be an ideal of R. Show that $f(A) = \{x \in R' \mid \exists\, a \in A, x = f(a)\}$ is an ideal of f(R).

RINGS – IV

Objectives

I. Maximal Ideals
II. Prime Ideal
III. Euclidean and Factorization Domains
III.(a) Euclidean Domains
III.(b) Principal Ideal Domain
IV. Prime and Irreducible Elements
V. Unique Factorization Domains
VI. Self Check Exercise

I. Maximal Ideals

Definition : Let R be a ring. An ideal $M \neq R$ of R is called a maximal ideal of R it whenever A is an ideal of R s.t., $M \subseteq A \subseteq R$ then either $A = M \text{ or } A = R$.

For Example : 1. A field F has only two ideals F and {0}. It is easy to see then that {0} is the only maximal ideal of F.

2. Let <E, +, . > be the ring of even integers.
Let $H_4 = \{4n \mid n \text{ an integer}\}$
then H_4 is an ideal of E and as $2 \notin H_4, H_4 \neq E$.

Let A be any ideal of E, s.t., $H_4 \subseteq A \subseteq E$

Suppose $H_4 \neq A$. We show A = E.

Since $H_4 \subset A, \exists$ some $x \in A$ s.t., $x \notin H_4$

By division algorithm, we can write
x = 4q + r where 0 < r < 4

Note r = 0 would mean $x = 4q \in H_4$. But $x \notin H_4$ so $r \neq 0$. Again, r = 1, 3 would imply x is odd which is not true. Hence the only value that r can have is 2.

Thus $x = 4q + 2 \Rightarrow 2 = x - 4q \in A$

$\text{as } x \in A, 4q \in H_4 \subseteq A \Rightarrow x - 4q \in A$

$2 \in A \Rightarrow$ members of the type 2 + 2, 2 + 2 + 2, ..., 0 – 2 are all in A

$\Rightarrow E \subseteq A$. But $A \subseteq E$

Hence A = E and H_4 is, therefore, a maximal ideal of E.

Problem 1 : Let R = Z[i] = {a + ib | a, b ∈ Z}. Let M = < 2 + i > then show that M is a maximal ideal of R.

Solution : Let $M \subseteq < a + bi > \subseteq R$

Then $2 + i = (a + bi)(c + di)$

$2 - i = (a - bi)(c - di)$

So $5 = (a^2 + b^2)(c^2 + d^2)$

If $a^2 + b^2 = 1$, then a = ±1, b = 0 or a = 0, b = ±1

Thus, a + bi = ±1 or ± i. In each case, a + bi is a unit, so <a + bi > = R.

If $c^2 + d^2 = 1$, then c = ±1, d = 0 or c = 0, d = ±1

Thus 2 + i = ± (a + bi) or (± i) (a + bi)

$\Rightarrow (a + bi) = (\pm 1)^{-1}(2 + i)$ or $(\pm 1)^{-1}(2 + i)$

In each case $a + bi \in < 2 + i >$

So $< a + bi > \subseteq < 2 + i > = M \subseteq < a + bi >$

$\Rightarrow M = < a + bi >$

Hence M is a maximal ideal of R.

Theorem 1 : Let R be a commutative ring with unity. An ideal M of R is maximal ideal of R iff $\frac{R}{M}$ is a field.

Proof : Let M be maximal ideal of R. Since R is commutative ring with unity, $\frac{R}{M}$ is also a commutative ring with unity. Thus all that we need prove is that non zero element of $\frac{R}{M}$ have multiplicative inverse.

Let $x + M \in \frac{R}{M}$ be any non zero element

then $x + M \neq M \Rightarrow x \notin M$

Let $xR = \{xr \mid r \in R\}$

It is easy to verify that xR is an ideal of R. Since sum of two ideals is an ideal, M + xR will be an ideal of R.

Again as $x = 0 + x.I \in M + xR$ and $x \notin M$ we find

$$M \subset M + xR \subseteq R$$

M maximal $\Rightarrow M + xR = R$

Thus $I \in R \Rightarrow 1 \in M + xR$

$\Rightarrow 1 = m + xr$ for some $m \in M, r \in R$

$\Rightarrow 1 + M = (m + xr) + M$

$= (m + M) + (xr + M) = xr + M$

$= (x + M)(r + M)$

$\Rightarrow (r + M)$ is multiplicative inverse of x + M

Hence $\frac{R}{M}$ is a field.

Conversely, let $\frac{R}{M}$ be a field.

Let I be any ideal of R s.t., $M \subseteq I \subseteq R$

then $\exists$ some $a \in I, s.t., a \notin M$

Now $a \notin M \Rightarrow a + M \neq M \Rightarrow a + M$ is a non zero element of $\frac{R}{M}$, which being a field, means a + M has multiplicative inverse. Let b + M be its inverse. Then

$$(a + M)(b + M) = 1 + M$$

$\Rightarrow ab + M = 1 + M$

$\Rightarrow ab - 1 \in M$

$\Rightarrow ab - 1 = m$ for some $m \in M$

$\Rightarrow 1 = ab - m \in I$ (using def. of ideal)

$\Rightarrow 1 = R$ (iedal containing unity, equals the ring)

Hence M is maximal ideal of R.

Remarks : (i) $\frac{R}{M}$ being a field contains at least two elements and thus unity and zero elements of $\frac{R}{M}$ are different i.e., $0+M \neq 1+M$ i.e, $I \notin M$ or that $M \neq R$.

(ii) In the converse part of the above theorem we do nto require R to have unity or it to be commutative, i.e., if R is a ring and M is ideal of R s.t., $\frac{R}{M}$ is a field then M is maximal.

Suppose I is an ideal of R s.t., $M \subset I \subseteq R$. Then $\exists a \in I, s.t., a \notin M$

Now $a \notin M \Rightarrow a+M \neq M \Rightarrow a+M$ is non zero element of $\frac{R}{M}$ and therefore has multiplicative inverse, say, b + M. If c + M be unity of $\frac{R}{M}$. (Not $\frac{R}{M}$ can have unity even if R doesn't have unity).

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

$\Rightarrow$ ab + M = c + M

$\Rightarrow$ $c - ab \in M \subset I$

But $a \in I \Rightarrow ab \in I$ and so (c – ab) + ab $\in$ I

$\Rightarrow$ $c \in I$

Let r $\in$ R be any element

Then $(r+M)(c+M) = r+M$

$\Rightarrow$ $rc + M = r + M$

$\Rightarrow$ $r - rc \in M \subset I$

Since $c \in I, rc \in I$ and thus $(r-rc)+rc \in I \Rightarrow r \in I \Rightarrow R \subseteq I$.

Hence I = R and thus M is maximal ideal of R.

(iii) Again, the condition of commutativity is essential in the theorem is established by the fact that we can have M, a maximal ideal in R where R/M is not a field and R is a non commutative ring with unity.

Cor.: A commutative ring R with unity is a field iff it has ano proper (non trivial) ideals.

If R is a field then it has no proper ideals.

Conversely, if R has no proper ideals then {0} must be a maximal ideal. Thus $\frac{R}{\{0\}}$ is a field and as $\frac{R}{\{0\}} \cong R, R$ is a field.

Problem 2 : Let R be the ring of n × n matrices over reals. Show that R has only two ideals namely {0} and R. Hence show that {0} is maximal ideal of R.

Solution : Let J be a non zero ideal of R. Let A be a non zero matrix in J. Since A ≠ 0, it has some non zero entry. Suppose $A = (a_{ij})$ and suppose $a_{rs} \neq 0$ in A.

If E_{ij} denotes the unit matrix in R whose (i, j)the entry is 1 and 0 elsewhere

then $E_{ij}E_{kr} = 0$ if $j \neq k$

$= E_{ir}$ if $j = k$

Now $A = a_{11}E_{11} + a_{12}E_{12} + ... + a_{nn}E_{nn}$

Consider $E_{ir}A\,E_{si} = E_{ir}\left(a_{11}E_{11} + a_{12}E_{12} + ... + a_{nn}E_{nn}\right)E_{si}$

$= E_{ir}\left(a_{rs}E_{rs}\right)E_{si}$

$= a_{rs}E_{ir}E_{si}$

$= a_{rs}E_{ii} \in J$ as $A \in J$ $\forall i$

So $\left(a_{rs}^{-1}E_{ij}\right)\left(a_{rs}E_{ij}\right) \in J$

$\Rightarrow E_{ii} \in J$ $\forall i = 1, 2, 3, ...n$

Thus identity matrix I in R can be written as $I = E_{11} + E_{12} + ... + E_{nn} \in J$.

So untiy of R belongs to J or that J = R. Hence {0} and R are the only ideals of R and so {0} is maximal ideal of R.

Note : Since $R \cong \frac{R}{\{0\}}$, and R is not a field, we find $\frac{R}{\{0\}}$ is not a field even through {0} is maximal.

II. Prime Ideal

Definition : An ideal P of a ring R is called a prime ideal if $ab \in P \Rightarrow a \in P$ or $b \in P$.

For Example: 1. $\{0\}$ in the ring Z of integers is a prime ideal as

$ab \in \{0\} \Rightarrow ab = 0 \Rightarrow a = 0 \text{ or } b = 0$

$\Rightarrow a \in \{0\} \text{ or } b \in \{0\}$

It is an example of a prime ideal which is not maximal.

2. $H_4 = \{4n \mid n \in Z\}$ which is a maximal ideal in the ring E of even integers.

H_4, however, is not a prime ideal as $2.2 = 4 \in H_4$ but $2 \notin H_4$.

In fact, H_4 is neither a maximal nor a prime ideal in Z.

Theorem 2 : Let R be a commutative ring. An ideal P of R is prime iff $\frac{R}{P}$ is an integral domain.

Proof : Let P be a prime ideal of R

Let $(a + P)(b + P) = 0 + P$

Then $ab + P = P$

$\Rightarrow ab \in P$

$\Rightarrow a \in P \text{ or } b \in P$

$\Rightarrow a + P = P \text{ or } b + P = P$

thus $\frac{R}{P}$ is integral domain.

Conversely, let $\frac{R}{P}$ be an integral domain.

Let $ab \in P$ then $ab + P = P$

$\Rightarrow (a + P)(b + P) = P$

$\Rightarrow a + P = P \text{ or } b + P = P$ (R/P is an integral domain)

$\Rightarrow a \in P \text{ or } b \in P$

Hence the result.

Theorem 3 : Let R be a commutative ring. An ideal P of R is a prime ideal if and only if for two ideals A, B of R, AB $\subseteq$ P implies either A $\subseteq$ P or B $\subseteq$ P.

Proof : Let P be a prime ideal of R and let AB $\subseteq$ P for two ideal A, B of R.

Suppose $A \not\subset P$ then $\exists$ some element $a \in A$ s.t., $a \notin P$.

Since $AB \subseteq P$, we get in particular

$$aB \subseteq P$$

$$\Rightarrow ab \in P \text{ for all } b \in B$$

Since P is prime, we get either $a \in P$ or $b \in P$ but $a \notin P$, hence $b \in P$ for all $b \in B$.

$$\Rightarrow B \subseteq P$$

Conversely, we show P is prime. Let $ab \in P$.

Let A and B be the ideals generated by a and b then A = (a), B = (b). If $x \in AB$ is any element then it is of the type

$$x = a_1b_1 + a_2b_2 + \ldots\ldots + a_nb_n \quad a_i \in A, b_i \in B$$

$$= (\alpha_1 a)(\beta_1 b) + (\alpha_2 a)(\beta_2 b) + \ldots. + (\alpha_n a)(\beta_n b)$$

for $\alpha_i, \beta_i \in R$ as $a_i \in A = (a), b_i \in B = (b)$

Thus $$x = (\alpha_1\beta_1)(ab) + (\alpha_2\beta_2)(ab) + \ldots\ldots + (\alpha_n\beta_n)(ab)$$

(R is commutative)

$$x = (\alpha_1\beta_1 + \alpha_2\beta_2 + \ldots. + \alpha_n\beta_n)ab$$

Since $ab \in P$, P is an ideal, all multiplies of ab are in P. Thus $x \in P$

i.e., $AB \subseteq P$

$$\Rightarrow A \subseteq P \text{ or } B \subseteq P$$

$$\Rightarrow (a) \subseteq P \text{ or } (b) \subseteq P$$

$$\Rightarrow a \in P \text{ or } b \in P \Rightarrow P \text{ is prime.}$$

Problem 3 : Let R be a non zero commutative ring with unity. If every ideal of R is prime show that R is a field and conversely.

Solution : To show that R is a field, we need show that every non zero element of R has multiplicative inverse. We first show that R is an integral domain.

Let $a, b \in R$ st., $ab = 0$

Then $ab \in \{0\}$ which is an ideal of R and is, therefore, prime ideal

$$\Rightarrow a \in \{0\} \text{ or } b \in \{0\}$$

i.e., a = 0 or b = 0

thus R is an integral domain.

Let now $a \in R$ be any non zero element and let

$$a^2R = \{a^2r \mid r \in R\}$$

then a^2R is an ideal of R (Verify !) and is therefore prime ideal.

Now $a \cdot a = a^2 = a^2 \cdot I \in a^2R$

$\Rightarrow a \in a^2R$

$\Rightarrow a = a^2b$ for some $b \in R$

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

$\Rightarrow 1 - ab = 0$ as $a \neq 0$

$\Rightarrow$ b is multiplicative inverse of a.

Hence R is a field.

Converse follows easily as a field R has no ideals except {0} and R.

Problem 4 : Let R be a commutative ring with unity. Show that every maximal ideal of R is prime.

Solution : We know that an ideal M of R is maximal iff $\frac{R}{M}$ is a field.

Thus if M is maximal, then $\frac{R}{M}$ is a field and hence an integral domain.

$\Rightarrow$ M is a prime ideal (theorem 2).

III. Euclidean and Factorization Domains

In order to understand the concept of Euclidean domains, Principal Ideal Domains (PIDs) and Unique Factorization domains, we first introduce some basic terms as discussed in the following.

Definition : Let R be a commutative ring.. a, b $\in$ R, $a \neq 0$, then we say a | b (a divides b) if $\exists$ c $\in$ R s.t., b = ac. Aslo then a is called a factor of b.

If a, b $\in$ R then an element d $\in$ R is called greatest common divisor (or highest common factor) of a and b if

(i) d | a, d | b

(ii) whenever c | a, c | b then c | d

and in that case we write d = g.c.d (a, b). In fact sometimes only (a, b) is used to denote g.c.d of a and b

Remark : One can prove that

(i) If $a|b$, $b|c$ thenf $a|c$

(ii) If $a|b$, $a|c$ then $a|b \pm c$

(iii) If $a|b$ then $a|bx$ for all $x \in R$

(iv) If R has unity then $1|x$ for all $x \in R$ and if a is a unit then $a|x$ for all $x \in R$.

For Example : 1. Consider the ring, R = {0, 1, 2, ..., 7} modulo 8

then since $2 \otimes 3 = 6$, $2|6$

$2 \otimes 2 = 4$, $2|4$

Again, if $c|4$, $c|6$ then $c|6 - 4 \Rightarrow c|2$

Thus g.c.d. (4, 6) = 2

Also $6 = 6 \otimes 1$, $4 = 6 \otimes 6$

we find $6|6$ and $6|4$

Now if $c|6$, $c|4$

then as $c|6$, we get g.c.d. (4, 6) = 6. Thus it is possible to have more than one g.c.d for the same pair of elements.

2. In the ring E of even integers we notice 4 and 6 do not have a g.c.d.

2(the only possibility) is not a g.c.d of 4, 6 as 2 6 in E. Indeed 6 = 2.3 but then $3 \notin E$. Of course, 2 is the unique g.c.d of 4 and 6 in Z, the ring of integers.

Definition : Let R be a commutative ring. A non zero element $l \in R$ is called least common multiple (l.c.m) of two (non zero) elements a, $b \in R$ of

(i) $a|l$, $b|l$

(ii) if $a|x$, $b|x$ then $l|x$

We denote l by l.c.m (a, b) = [a, b]

Note that a pair of elements in a ring may not have an l.c.m. and a pair could have more than one l.c.m.

Definition : Let R be a commutative ring with unity. Then a, $b \in R$ are called associates if b = ua for some unit u in R.

We recall here that by a unit we mean an element which has multiplicative inverse. The above definition will not be 'complete' unless we show that the relation 'is an associate of' is an equivalence relation. If we denote the relation by ~.

then $a \sim a$ as $a = 1.a$ and 1 is a unit

$a \sim b \Rightarrow b = ua$ where u is a unit

$\Rightarrow u^{-1} b = a$

$\Rightarrow b \sim a$

Indeed u^{-1} will be a unit if u is a unit.

Finally $a \sim b$, $b \sim c \Rightarrow b = ua$

$c = vb$ for units u, v

Since $c = vb = v(ua) = (vu)\, a$

showing $c \sim a$

as $uu^{-1} = 1$, $vv^{-1} = 1 \Rightarrow (vu)(vu)^{-1} = (vu)\,(u^{-1}v^{-1}) = 1$

we notion vu is a unit.

For Example : 3i – 4 is an associate of 4i + 3 in complex nos.

Problem 5 : Let R be an integral domain with unity and a, b $\in$ R be non zero elements such that a/b and b/a, then a and b are associates and conversely.

Solution : $a \mid b \Rightarrow b = xa$

$b \mid a \Rightarrow a = yb$ for some x, y $\in$ R

$\therefore$ $b = xa = x(yb)$

$\Rightarrow b(1 - xy) = 0$

$\Rightarrow 1 - xy = 0$ as $b \neq 0$

$\Rightarrow$ y is unit in R and a = yb, and thus a, b are associates

Conversely, if a, b are associates then $\exists$ a unit u, s.t., a = bu (and so $au^{-1} = b$).

$\Rightarrow b \mid a$ and $a \mid b$.

Theorem 4 : Let R be an integral domain with unity. If d_1 = g.c.d (a, b) in R then d_2 is also a g.c.d (a, b) iff d_1 and d_2 are associates.

Proof : One may remark here that we prove this result only after assuming the existence of g.c.d.

Let d_1 and d_2 be both g.c.d (a, b).

Then $d_1 \mid a, d_1 \mid b$

and $d_2 \mid a, d_2 \mid b$

by definition, we get $d_1 \mid d_2$ and $d_2 \mid d_1$

$\Rightarrow d_1$ and d_2 are associates (using problem 5)

Conversly, let d_1 = g.c.d. (a, b) and d_2 be an associate of d_1.

Then $ud_2 = d_1$ for some unit u

$\Rightarrow d_2 \mid d_1$ and as $d_1 \mid a, d_1 \mid b$

we find $d_2 \mid a$ and $d_2 \mid b$

Let $x \mid a, x \mid b$ then $x \mid d_1$ as b_1 is g.c.d. (a, b)

Also as $d_2 = d_1 u^{-1}$

$d_1 \mid d_2$

and thus $x \mid d_2$

$\Rightarrow d_2 = \text{g.c.d}(a, b)$

Theorem 5 : Let R be an integral domain with unity. If l_1 = l.c.m (a, b) in R then l_2 is also an l.c.m (a, b) iff l_1 and l_2 are associates.

Proof : Try Yourself.

Problem 6 : Let R be an integral domain with unity. If g.c.d (a, b) = d for a, b ∈ R then cd and g.c.d (ca, cb) are associates.

Solution : Let g.c.d. (ca, cb) = d'

Since $d|a$, $a = dk$

$\Rightarrow ac = dkc = cdk$

$\Rightarrow cd|ca$

Similarly $cd|cb \Rightarrow cd|d' \Rightarrow d' = cdt$

Again $d'|ca \Rightarrow ca = d's$

$\Rightarrow ca = d's \Rightarrow cdts$

$\Rightarrow a = (dt)s \Rightarrow dt|a$

Similarly $dt|b$

$\Rightarrow dt|d \Rightarrow d = dtp \Rightarrow d(1 - tp) = 0$

$\Rightarrow 1 = tp \Rightarrow t$ is a unit

$\Rightarrow$ g.c.d. (ca, cb) = d' = cdt

i..e, cd and d' are associates.

III.(a) Euclidean Domains

Defintion : An integral domain R is called a Euclidean domain (or a Euclidean ring) if for all $a \in R$, $a \neq 0$ there is defined a non –ve integer d(a) s.t.,

(i) for all $a, b \in R, a \neq 0, b \neq 0, d(a) \leq d(ab)$

(ii) for all $a, b \in R, a \neq 0, b \neq 0, \exists$ t and r in R s.t.,

$a = tb + r$

where either r = 0 or d(r) < d(b).

For Example : Consider the integral domain < Z, +, □> of integers. For any $0 \neq a \in Z$, define d(a) = |a|, then d(a) is non –ve integer.

Again, let a, b ∈ Z be any element s.t., a ≠ 0, b ≠ 0

then $d(a) = |a|$

$d(ab) = |ab| = |a||b|$

thus $d(a) \leq d(ab)$ as $|a| \leq |a||b|$

Again let a, b ∈ Z (a, b ≠ 0)

Suppose b > 0, then it is possible to write

$a = tb + r$ where $0 \leq r < b$

t, r ∈ Z

If r ≠ 0 then $r < b \Rightarrow |r| < |b|$

$\Rightarrow d(r) < d(b)$

If $b < 0$, then $(-b) > 0$,

$\therefore \exists\, t, r \in Z$ s.t.

$a + (-b)t + r = (-t)b + r$

where $0 \le r < -b$

and if $r \ne 0, r < -b$

$\Rightarrow |r| < |b|$

$\Rightarrow d(r) < d(b)$

Hence < Z, +, □> is a Euclidean domain.

Remarks : (i) When we say, in the definiton, that ∃ a non-ve integer d(a) for any 0 ≠ a, we mean, ∃ a function d from R – {0} to $Z^+ \cup \{0\}$ where Z^+ is set of ve integers. This function d is called Euclidean valuation or R. Also the last condition in the definition is called Euclidean algorithm.

(ii) We can show that the t and r mentioned in the last (Euclidean algorithm) condition in the definition of Euclidean domain are uniquely determined iff

$$d(a+b) \le \text{Max.}\{a(a), d(b)\}$$

Let $d(a+b) \le \text{Max.}\{d(a), d(b)\}$ and

Suppose $a = tb + r = t_1 b + r_1$

Let $r_1 - r \ne 0$, then $b(t - t_1) = r_1 - r \ne 0$, and so $t - t_1 \ne 0$

Now $d(b) \le d(b(t - t_1))$

$= d(r_1 - r)$

$\le \text{Max.}\{d(r_1), d(-r)\}$ (given condition)

$= \text{Max.}\{d(r_1), d(-r)\}$

< d(b) which is not possible.

Thus $r_1 - r = 0 \Rightarrow b(t - t_1) = 0$

or $t - t_1 = 0$ as $b \ne 0$

$\Rightarrow$ $t - t_1$ and $r = r_1$

Conversely, let t, r be uniquely determined and suppose

$$d(a+b) > \text{Max.}\{d(a), d(b)\} \text{ for some a, b (non zero) in R.}$$

Now $b = 0(a+b) + b = 1.(a+b) - a$

Also $d(-a) = d(a) < d(a+b)$

and $d(b) < d(a+b)$

Thus for $b, 1 \in R, \exists t = 0, r = b \text{ or } t_1 = 1, r_1 = -a \text{ s.t.}, b = t.1 + r, b = t_1.1 + r_2$

where $r \neq r_1 (\text{as } a + b \neq 0) t \neq t_1$, a contradiction to the uniquencess.

Hence $d(a+b) \leq \text{Max.}(d(a), d(b))$. Note that a Euclidean domain contains unity.

Theorem 6 : Let R be a Euclidean domain and let A be an ideal of R, then $\exists\, a_0 \in A$ s.t., $A = \{a_0 x \mid x \in R\}$.

Proof : If A = {0}, we can take $a_0 = 0$.

Suppose $A \neq \{0\}$, then $\exists$ at least one $0 \neq a \in A$.

Let $a_0 \in A$ be such that $d(a_0)$ is minimal [Existence is ensured by the well ordering principle which states that every non empty subset of non –ve integers has least element.]

We claim A is generated by this a_0.

Let $a \in A$, $a \neq 0$ then by definition, $\exists$ t, r $\in$ R, s.t.,

$$a = a_0 t + r \text{ where either } r = 0 \text{ or } d(r) < d(a_0)$$

Suppose $r \neq 0$

Then $a_0 \in A, t \in R \Rightarrow ta_0 \in A$

$$a \in A, ta_0 \in A \Rightarrow a - ta_0 \in A$$

$$\Rightarrow r \in A$$

But $d(a_0)$ is the smallest d-value in A and $d(r) < d(a_0)$, which leads to a contradiction.

Hence r = 0

$$\Rightarrow a = ta_0$$

Thus any $a \in A$ can be put in the form ta_0

$$\Rightarrow A \subseteq \{a_0 x \mid x \in R\}$$

But $\{a_0 x \mid x \in R\} \subseteq A$ as $a_0 \in A \Rightarrow xa_0 \in A$ for all $x \in R$

Hence $A = \{a_0 x \mid x \in R\}$

which proves the theorem.

Definition : Such an ideal A which contains multiples of an element a_0, including a_0 of R is called a Principal Ideal of R, generated by a_0. We denote this by $A = (a_0)$.

In other words, the smallest ideal of R which contains a_0 is called Principal Ideal generated by a_0.

In view of this definition the previous theorem will read as

Theorem 6 : Every ideal in a Euclidean domain is a principal ideal.

Cor.: A Euclidean domain possesses unity.

Proof : Let R be a Euclidean domain then R is its own ideal and, therefore, R is generated by some element r_0 of R.

Thus each element of R is a multiple of r_0.

In particular r_0 is a multiple of r_0

i.e., $r_0 = r_0 k$ for some $k \in R$

Now if $a \in R$ is any element then as $R = (r_0)$

$$a = x r_0 \text{ for some } x$$

hence $ak = (x r_0)\, k = x(r_0 k) = x r_0 = a$

i.e., k is unity of R.

III.(b) Principal Ideal Domain

Definition : An integral domain R with unity is called a Principal Ideal Domain (PID) if every ideal of R is a principal ideal.

In fact, if R happens to be a commutative ring with unity with above condition, we call it a principal ideal ring.

In view of the previous theorem and cor., we get

Theorem 7 : A Euclidean domain is a PID.

In particular thus, the ring <Z, +, .> of integers is a PID. This result follows independently from the fact that every ideal in <Z, +, .> is a principal ideal.

Remarks : (i) A field F is always a PID as it has only two ideals F and {0}. F is generated by 1 and {0} by 0.

(ii) One can show that there exist PIDs which are not Euclidean domains. IN particular, $Z\left[\sqrt{-19}\right] = \left\{a + \sqrt{-19}\, b \mid a, b \in Z\right\}$ where a, b are both odd or both even, is a PID but not a Euclidean domain.

Problem 7 : Show that in a PID every non-zero prime ideal is maximal.

Solution : Let P = (p), $p \neq 0$, be a non zero prime ideal in a PID R.

Suppose $P \subseteq Q = (q) \subseteq R$

Then $p \in P \subseteq Q = (q)$

$\Rightarrow p = qr$

$\Rightarrow qr \in P$

$\Rightarrow q \in P$ or $r \in P$

If $q \in P$ then all multiples of q are in $P \Rightarrow Q \subseteq P$

thus $Q = P$

If $r \in P$ then $r = pt \Rightarrow r = qrt$

$\Rightarrow r(1 - qt) = 0$

$\Rightarrow 1 - qt \ (r \neq 0)$

But $q \in Q, t \in R \Rightarrow qt \in Q \Rightarrow 1 \in Q \Rightarrow Q = R$

Note r = 0 would mean $p = q \,.\, 0 \Rightarrow p = 0 \Rightarrow P = (0)$.

Problem 8 : Show that $Z\left[\sqrt{2}\right] = \left\{a + \sqrt{2}b \mid a, b \in Z\right\}$ is a Euclidean domain.

Solution : It is easy to see that $Z\left[\sqrt{2}\right]$ is an integral domain. Define a mapping

$d : Z\left[\sqrt{2}\right] - \{0\} \to Z$ by

$$d\left(a + \sqrt{2}b\right) = |\, a^2 - 2b^2 \,|$$

then $\left|a^2 - 2b^2\right| \geq 1$ as $a^2 - 2b^2 = 0 \Rightarrow \sqrt{2} = \dfrac{a}{b}$ which is not possible.

Again, $d\left[\left(a + \sqrt{2}b\right)\left(c + \sqrt{2}d\right)\right] = d\left[(ad + 2bd) + \sqrt{2}\,(ad + bc)\right]$

$$= \left|(ac + 2bd)^2 - 2(ad + bc)^2\right|$$

$$= \left|\left(a^2 - 2b^2\right)\left(c^2 - 2d^2\right)\right|$$

$$= \left|a^2 - 2b^2\right| \left|c^2 - 2d^2\right| \qquad \ldots (1)$$

$$\geq \left|a^2 - 2b^2\right| = d\left(a + \sqrt{2}b\right)$$

i.e., $d\left(a + \sqrt{2}b\right) \leq d\left[\left(a + \sqrt{2}b\right)\left(c + \sqrt{2}\, d\right)\right]$

Let now $a + \sqrt{2}b$ and $c + \sqrt{2}d$ be two members of $Z\left(\sqrt{2}\right)$ and suppose $c + \sqrt{2}\, d \neq 0$, then

$$\frac{a + \sqrt{2}b}{c + \sqrt{2}d} = \frac{\left(a + \sqrt{2}b\right)\left(c - \sqrt{2}d\right)}{c^2 - 2d^2} = \frac{ac - bd}{c^2 - 2d^2} + \frac{\sqrt{2}\left(bc - ad\right)}{c^2 - 2d^2}$$

$$= m + \sqrt{2}\, n \,(\text{say})$$

then m and n are rationals.

Now $m = [m] + \theta$ where [m] is the greatest integer not greater than m and θ is fractional part of m.

If $0 \leq \theta \leq \frac{1}{2}$, take $p = [m]$

and if $\frac{1}{2} < \theta < 1$, take $p = [m] + 1$

Thus $\exists$ an integer p, s.t., $|m - p| \leq \frac{1}{2}$

Similarly we can find an integer q, s.t., $|n - q| \leq \frac{1}{2}$

Put $m - p = \alpha, n - p = \beta$, then $|\alpha| \leq \frac{1}{2}, |\beta| \leq \frac{1}{2}$

Also then $= \frac{a + \sqrt{2}b}{c + \sqrt{2}d} = (p + \alpha) + \sqrt{2}\,(q + \beta)$

$$\Rightarrow \frac{a + \sqrt{2}b}{c + \sqrt{2}d} = \left(p + \sqrt{2}q\right) + \left(\alpha + \sqrt{2}\beta\right)$$

$$\Rightarrow a+\sqrt{2}b=\left(c+\sqrt{2}d\right)\left(p+\sqrt{2}q\right)+\left(c+\sqrt{2}d\right)\left[(m-p)+\sqrt{2}\,(n-q)\right]$$

where, of course, $\left(p+\sqrt{2}q\right)\in Z\left[\sqrt{2}\right]$ as p, q are integers

we can thus write

$$a+\sqrt{2}b=\left(c+\sqrt{2}d\right)\left(p+\sqrt{2}q\right)+r$$

where $r=\left(c+\sqrt{2}d\right)\left[(m-p)+\sqrt{2}\,(n-q)\right]$

and as $r=\left(a+\sqrt{2}b\right)-\left(c+\sqrt{2}d\right)\left(p+\sqrt{2}q\right)$

we notice $r\in Z\left[\sqrt{2}\right]$

Now if $r\neq 0, d(r)=d\left[\left(c+\sqrt{2}d\right)\left\{(m-p)+(n-q)\sqrt{2}\right\}\right]$

$$=d\left[\left(c+\sqrt{2}d\right)\right]\left[d\left((m-p)+\sqrt{2}\,(n-q)\right)\right]$$

[using (1) one may notice here that in proving (1) we do not essentially require that a, b, c, d are integers]

$$\Rightarrow d(r)=|c^2-2d^2||(m-p)^2-2(n-q)^2|$$

$$=|c^2-2d^2||(m-p)^2+2(n-q)^2|$$

$$\leq|c^2-2d^2|\left|\frac{1}{4}+\frac{2}{4}\right|$$

$$\leq|c^2-2d^2|=d\left(c+\sqrt{2}d\right)$$

Hence, for $a+\sqrt{2}b, c+\sqrt{2}d\in Z\left[\sqrt{2}\right]\exists\, p+\sqrt{2}q, r\in Z\left[\sqrt{2}\right]$ s.t.,

$$\left(a+\sqrt{2}b\right)=\left(c+\sqrt{2}d\right)\left(p+\sqrt{2}d\right)+r$$

where either $r=0$ or $d(r)<d\left(c+\sqrt{2}d\right)$

showing that $Z\left[\sqrt{2}\right]$ is a Euclidean domain.

Theorem 8 : Let a, b be two non zero elements of a Euclidean domain R. If b is not a unit in R then d(a) < d (ab).

Proof : Let b be not a unit. Then for a, ab in R $\exists$ t, r $\in$ R s.t.,

$$a = tab + r$$

where either r = 0 or d(r) < d(ab)

If $r = 0$, then $a = tab \Rightarrow a(1 - t\,b) = 0$

$\Rightarrow tb = 1$ or that b is a unit, which is not so.

Thus $r \neq 0$ and $d(r) < d(ab)$

Now $r = a - tab = a(1 - tb)$

Hence $d(a) \leq d(a(1 - tb)) = d(r) < d(ab)$.

Cor.: If a, b are non zero elements of a Euclidean domain R then d(a) = d(ab) iff b is a unit.

If b is a unit then $\exists$ c s.t., bc = 1

Now $d(a) \leq d(ab) \leq d((ab)c) = d(a)$

$\Rightarrow d(a) = d(ab)$

Converse follows from above theorem.

Problem 9 : Show that an element x in a Euclidean domain is a unit of and only if d(x) = d(1).

Solution : Let d(x) = d(1)

Suppose x is not a unit, then by above theorem

$d(1) < d(1 \cdot x)$ Taking a = 1, b = x

i.e., $d(1) < d(x)$

a contradiction

$\therefore$ x is a unit.

Conversely, let x be a unit in R, then $\exists$ y $\in$ R s.t.,

$$xy = 1$$

Now $d(x) \leq d(xy)$ (by definition)

$\Rightarrow d(x) \leq d(1)$

Also $d(1) \leq d(1 \cdot x)$

$\Rightarrow d(1) \leq d(x)$

Hence $d(x) = d(1)$.

IV. Prime and Irreducible Elements

In an integral domain R with unity, a b (non zero) are said to be co-prime or relatively prime, if g.c.d. (a, b) is a unit in R.

Definition : Let R be a commutative ring with unity. An element $p \in R$ is called a prime element if

(i) $p \neq 0$, p is not a unit.

(ii) For any $a, b \in R$, if $p \mid ab$ then $p \mid a$ or $p \mid b$.

Let R be a commutative ring with unity. An element $p \in R$ is called an irreducible element if

(i) $p \neq 0$, p is not a unit.

(ii) whenever p = ab then one of a or b must be a unit. (In other words, p has no proper factors.)

For example : In the ring $< Z, +, \square >$ of integers, every prime number is a prime element as well as irreducible element.

Problem 10 : Find all the units of $Z\left[\sqrt{-5}\right]$.

Solution : Suppose $a + \sqrt{-5}b$ is a unit in $Z\left[\sqrt{-5}\right]$.

Then $\left(a + \sqrt{-5}b\right)\left(c + \sqrt{-5}d\right) = 1 + \sqrt{-5}\,.\,0$ for some $c, d \in Z$

So, $\left(a - \sqrt{-5}b\right)\left(c - \sqrt{-5}d\right) = \overline{1} = 1$

giving $\left(a^2 + 5b^2\right)\left(c^2 + 5b^2\right) = 1$ in Z

$\Rightarrow \quad a^2 + 5b^2 = 1 \Rightarrow a = \pm 1, b = 0$

Thus $a + \sqrt{-5}b = \pm 1$ are the units in $Z\left[\sqrt{-5}\right]$.

Theorem 9 : In a PID an element is prime if and only if it is irreducible.

Proof : Let D be a PID and let $p \in D$ be a prime element. We need prove only that if p = ab, then a or b is a unit.

So let p = ab then $p \mid ab$

$\Rightarrow p \mid a$ or $p \mid b$ (p is prime)

If $p \mid a$ then a = px for some x

So $p = ab = (px)b$

$\Rightarrow p(1 - xb) = 0$

$\Rightarrow 1 - xb = 0$ as $p \neq 0$

$\Rightarrow xb = 1 \Rightarrow b$ is a unit.

Similarly, if p | b then a will be a unit.

Conversely, let p be irreducible element and suppose p | ab. We show either p | a or p | b.

If p | a, we have nothing to prove.

Suppose p + a

Since p, a are elements of a PID thye have a g.c.d., say, d.

We show d is a unit.

Now $d \mid p$ and $d \mid a$

$\Rightarrow \exists\, u, v$ s.t., $p = du$, $a = dv$

If d is not a unit then as p is irreducible and p = du, u will be a unit

$\Rightarrow$ u^{-1} exists

$\Rightarrow$ $pu^{-1} = d$

$\therefore$ $a = pu^{-1}v \Rightarrow p \mid a$ which is not so.

Thus d is a unit.

Again, we know that d can be expressed as

$$d = \lambda a + \mu p$$

which gives $dd^{-1} = d^{-1}\lambda a + d^{-1}\mu p$

$$\Rightarrow b.1 = \lambda d^{-1}ab + \mu d^{-1}bp$$

But $p \mid ab.p \mid \mu d^{-1}bp$

$\therefore$ $p \mid \left(ab\lambda d^{-1} + \mu d^{-1}bp\right)$

$$\Rightarrow p \mid b$$

Hence the result follows.

V. Unique Factorization Domains

Definition : Let R be an integral domain with unity then R is called a unique factorization domain (UFD) if

(i) everynon zero, non unit element a of R can be expressed as a product of finite number of irreducible elements of R and

(ii) if $a = p_1 p_2 \ldots p_m$

$a = q_1 q_2 \ldots q_n$

where p_i and q_j are irreducible in R then m = n and each p_i is an associate of some q_j.

For Example : 1. The ring <Z, +, . > of integers is a UFD. We know it is an integral domain with unity. If $n \in Z$ be any non zero, non unit element (i.e., $n \neq 0, \pm 1$) of Z then if n > 0, we can write

$$n = p_1^{\alpha_1} p_2^{\alpha_2} .....p_m^{\alpha_m} \text{ where } p_i \text{ are primes}$$

$$\Rightarrow n = (p_1 p_1 .....p_1)(p_2 p_2 .....p_2) .... (p_r p_r .....p_r)$$

or that n is a product of prime (and thus irreducible) elements of Z. Again this representation of n is unique (by Fundamental theorem of Arithmetic).

In case n < 0, let n = (–m) where m > 0 then we can express m as product of primes (therefore, irreducibles) in Z.

say, $m = q_1 q_2 ... q_k$

then $(-m) = n = (-q_1)(q_2) ..... (q_k)$

2. A field < F, +, . > is always a UFD as it contains no non zero, non unit elements.

3. $Z\left[\sqrt{-5}\right]$ is an integral domain which is not a UFD.

$46 \in Z\left[-\sqrt{5}\right]$ is a non unit, non zero element and we can express it as product of irreducibles in two ways

$$46 = 2.23$$

$$46 = \left(1 + 3\sqrt{-5}\right)\left(1 - 3\sqrt{-5}\right)$$

But 2 is not an associate of $1 + 3\sqrt{-5}$ or $1 - 3\sqrt{-5}$. Hence $Z\left[\sqrt{-5}\right]$ is not a UFD.

Theorem 10 : In a UFD R an element is prime iff it is irreducible.

Proof : Let $a \in R$ be a prime element, then since R is an integral domain with unity, a will be irreducible.

Conversely, let $a \in R$ be irreducible. Then a is non zero, non unit. Let a | bc then bc = ak for some k

Case (i) : b is a unit

then $c = akb^{-1} = a\left(kb^{-1}\right) \Rightarrow a \mid c.$

Case (ii) : c is a unit then similarly, a | b.

Case (iii) : b, c are non units

If k is a unit, then bc = ak

$$\Rightarrow a = b\left(ck^{-1}\right)$$

Since a is irreducible, either b or ck^{-1} is a unit. But b is not a unit. Thus ck^{-1} is a unit.

But that implies c is a unit, which is again not true. Hence k is not a unit.

We can thus express

$$b = p_1p_2 \ldots p_m$$

$$c = q_1q_2 \ldots q_n$$

$$k = r_1r_2 \ldots r_1$$

as product of irreducibles (by def. of UFD).

So bc = ak becomes

$$p_1p_2\ldots p_m\ q_1q_2\ldots q_n = ar_1\ r_2\ldots r_1 = x(\text{say})$$

Then x is an element having two representations as product irreducible elements. By Def. of UFD each element in one representation is an associate of some element in the other.

$\Rightarrow$ a is an associate of some p_i or some q_j

$\Rightarrow$ $ua = p_i$ or $ua = q_j$ for some unit u

$$\Rightarrow a \mid p_i \text{ or } a \mid q_j$$

$$\Rightarrow a \mid b \text{ or } a \mid c$$

$\Rightarrow$ a is prime element.

VI. Self Check Exercise

1. Show that intersection of two prime ideals may not be a prime ideal.

2. Let R be a commutative ring. Let I be an ideal of R and let P be a prime ideal of I. Show that P is an ideal of R.

3. Show that a commutative ring R is an integral domain iff {0} is a prime ideal.

4. In the ring of integers, show that every ideal if generated by some integer. Show further that an ideal is maximal iff it is generated by a prime.

5. Show that every field is a Euclidean domain.

6. In the ring $Z\left[\sqrt{-5}\right] = \left\{a + \sqrt{-5}b \mid a, b \in Z\right\}$, show that $1 + 3\sqrt{-5}$ is irreducible element but is not prime.

7. Show that in $Z\left[\sqrt{-3}\right], 1+\sqrt{-3}$ is irreducible but not prime element.

8. Show that $Z\left[\sqrt{3}\right] = \left\{a+\sqrt{3}b \mid a,b \in Z\right\}$ is a Euclidean domain.

9. Show that $Z\left[\sqrt{-3}\right]$ is not a UFD.

10. Show that in a UFD R, every non zero prime ideal ($\neq$ R) contains a prime element.