

# *The Rings(2)*

## *Fouth Class*

*By*

*Dr. Alaa Abbas*

## **CONTENTS:**

1. Certain special ideals.
2. The radicals of ideals.(semiprime and primary ideals).
3. The ring homomorphism of the radicals.
4. The Jacobson radicals of a ring with some basic properties.
5. The prime radicals of a ring with some basic properties.
6. The divisibility theory in integral domain.
7. The prime and irreducible elements.
8. The unique factorization domain.
9. The Euclidean domain.
10. The polynomial rings.
11. The division algorithm theorem.
12. The remainder theorem with some application.
13. Extensions of fields.
14. Kronecker's theorem with applications.
15. The Boolean ring and Boolean algebra.

## **REFERENCES:**

- 1) Burton D. M., "Introduction To Modern Abstract Algebra", 1967, London.
- 2) David M. Burton, WM. C. Brown Publishers "Abstract Algebra", 1988.

**Definition:**

A **ring** is an ordered triple  $(R, +, \cdot)$ , where  $R$  is a nonempty set and  $+, \cdot$  are two binary operation on  $R$  such that:

- 1)  $(R, +)$  is an abelian group.
- 2)  $(R, \cdot)$  is a semigroup and
- 3) The operation  $\cdot$  is distributive over the operation  $+$ .

**Example:**

If  $Z, Q, R^\#$  denote the sets of integers, rational, and real numbers, then the systems

$$(Z, +, \cdot), (Q, +, \cdot), (R^\#, +, \cdot).$$

Are all examples of rings; here  $+$  and  $\cdot$  are taken to be ordinary addition and multiplication.

**Definition:**

Let  $R$  be a commutative ring. An element  $a \in R$  is called **zero divisor** if  $a \neq 0$  and there exists  $b \in R, b \neq 0$  with  $a \cdot b = 0$ .

**Example:**

$$Z_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$$

**Solution:**  $\bar{2} \cdot \bar{3} = \bar{0}, \quad \bar{3} \cdot \bar{4} = \bar{0}, \quad \bar{2}, \bar{3}, \bar{4}$  are zero divisors of  $Z_6$ .

**Example:**

$Z_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$  Has no zero divisors.

**Definition:**

A commutative ring with identity is called an **integral domain** if it has no zero divisors.

**Example:**

$(Z, +, \cdot), (Q, +, \cdot), (R, +, \cdot), (Z_p, +_p, \cdot_p)$  Where  $p$  is prime are integral domains.

**Definition:**

A ring  $(R, +, \cdot)$  is said to be **field** if  $(R - \{0\}, \cdot)$  forms a commutative ring (with identity 1).

Or

The field is commutative ring with identity in which each nonzero element has inverse under multiplication.

**Definition:**

Let  $(R, +, \cdot)$  be a ring, and  $\emptyset \neq S \subseteq R$ , then  $(S, +, \cdot)$  is called a **subring** if  $(S, +, \cdot)$  is a ring itself.

**Example:**

$(2Z, +, \cdot)$  subring of  $(Z, +, \cdot)$

**Rremark:**

Let  $(R, +, \cdot)$  be a ring  $\emptyset \neq S \subseteq R$ , then  $(S, +, \cdot)$  is subring if:

$$(1) \ a - b \in S \quad \forall a, b \in S.$$

$$(2) \ a \cdot b \in S \quad \forall a, b \in S.$$

**Definition:**

A subring  $I$  of the ring  $R$  is said to be two sided **ideal** of  $R$  if and only if  $r \in R$  and  $a \in I$  imply  $ra \in I$  and  $ar \in I$ .

**Definition:**

Let  $I$  be a nonempty subset of ring  $R$ , then  $I$  is **ideal** of  $R$  if

$$(1) a - b \in I \quad \forall a, b \in I.$$

$$(2) ar \in I, (ra \in I) \quad \forall a \in I, r \in R.$$

**Remark:**

Every ideal is subring.

**Proof:** Let  $I$  be an ideal, to show that  $I$  is subring

$$(1) I \neq \emptyset$$

$$(2) \text{ Let } a, b \in I \Rightarrow a.b \in I, a - b \in I$$

$\therefore I$  is subring

But the converse is not true for example:

$(Q, +, \cdot)$  is a ring,  $Z \subseteq Q$ ;  $Z$  is subring

$$3 \in Z, \frac{1}{2} \in Q, 3 \cdot \frac{1}{2} = \frac{3}{2} \notin Z$$

$\therefore Z$  is not ideal

**Remark<sup>(\*)</sup>:**

Let  $I$  be an ideal of a ring with 1. If  $1 \in I$ , then  $I = R$ .

**Proof:**  $I \subseteq R$ , let  $r \in R, 1 \in I$  but  $I$  is ideal

$$\therefore 1.r \in I \Rightarrow r \in I \Rightarrow R \subseteq I.$$

Thus  $I = R$

**Remark:**

Let  $I$  be an ideal of a ring with 1 and  $I$  contains an invertible element, then  $I = R$ .

**Proof:**  $a \in I$  but  $a$  is invertible then  $\exists b \in R$  such that  $a \cdot b \in I \Rightarrow 1 \in I$

$\therefore I = R$ , by remark (\*)

**Definition:**

A ring  $R$  is called ***principle ideal ring*** if every ideal in  $R$  is principle ideal.

**Theorem:**

$(\mathbb{Z}, +, \cdot)$  is P. I. R.

**Proof:** (H.W)

**Definition:**

A proper ideal  $M$  of a ring  $R$  is called ***maximal ideal*** if where ever  $I$  is an ideal of  $R$  with  $M \subset I$ , then  $I = R$ .

**Example:**

In  $\mathbb{Z}_6$  the ideals are:

$$\{0\}, \mathbb{Z}_6, \{\bar{0}, \bar{3}\}, \{\bar{0}, \bar{2}, \bar{4}\}$$

$\{\bar{0}, \bar{3}\}$  is the maximal in  $\mathbb{Z}_6$ .

$\{\bar{0}, \bar{2}, \bar{4}\}$  is the maximal in  $\mathbb{Z}_6$ .

**Theorem:**

Let  $R$  be commutative ring with 1 and  $I$  be a proper ideal of  $R$ ,  $I$  is a maximal ideal if and only if  $\frac{R}{I}$  is a field.

**Proof:** (H.W)

**Definition:**

A proper ideal  $P$  of a ring  $R$  is called a **prime** ideal if for all  $a, b$  in  $R$  with  $a.b \in P$  either  $a \in P$  or  $b \in P$ .

**Example:**

1)  $4\mathbb{Z}$  is an ideal in  $\mathbb{Z}$ , but not a prime ideal in  $\mathbb{Z}$ .

2)  $\{0\}$  is a prime ideal in  $\mathbb{Z}$  but not maximal.

3)  $\{0\}$  is not a prime ideal in  $\mathbb{Z}_6$ .

**Theorem:**

Let  $R$  be commutative ring with 1 and  $P$  be a proper ideal of  $R$ ,  $P$  is a prime ideal if and only if  $\frac{R}{P}$  is an integral domain.

**Proof:** (H.W)

**Definition:**

A commutative ring with identity is called local ring if it has unique maximal ideal.

**Example:**

$\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$  is a local ring.

**Remark:**

Every field is a local ring

**Proof:** (H.W)

**Remark:**

In the local ring the idempotent element is only 0 or 1.

**Proof:** let  $a \neq 0$  and  $a \neq 1$  be an idempotent element. Since  $a$  is an idempotent, then  $a^2 = a$ , then  $a^2 - a = 0$ , then  $a(a - 1) = 0$ , since  $a \neq 0$  and  $a, a - 1$  are zero divisors, thus  $a, a - 1$  has no inverse, hence  $a, a - 1$  must belong to the unique maximal ideal say  $M$ , then  $a, a - 1 \in M$ , then  $a - (a - 1) \in M$ , hence  $1 \in M$ . Thus either  $a = 0$  or  $a = 1$ .

**Definition:**

Let  $I$  be an ideal of a ring  $R$ . Then the nil radical of  $I$  denoted by  $\sqrt{I}$  is the set:

$$\sqrt{I} = \{r \in R : \exists n \in \mathbb{Z}^+ \ni r^n \in I\}$$

**Remark(1):**

1.  $\sqrt{I} \supseteq I$ .
2.  $\sqrt{I}$  is an ideal of  $R$ .

**Proof:** (H.W)

**Remark(2):**

1.  $\sqrt{I \cap J} = \sqrt{IJ} = \sqrt{I} \cap \sqrt{J}$ .
2.  $\sqrt{\sqrt{I}} = \sqrt{I}$ .
3.  $\sqrt{I + J} \supseteq \sqrt{I} + \sqrt{J}$ .

**Proof:1)** Let  $w \in \sqrt{I \cap J}$ , then  $\exists n \in \mathbb{Z}^+ \ni w^n \in I \cap J$ , then  $w^n \in I$  and  $w^n \in J$ , hence  $w \in \sqrt{I}$  and  $w \in \sqrt{J}$ . Thus  $w \in \sqrt{I} \cap \sqrt{J}$ .



Let  $y \in \sqrt{I} \cap \sqrt{J}$ , then  $y \in \sqrt{I}$  and  $y \in \sqrt{J}$ , hence  $y^n \in I$  and  $y^n \in J$ .

$y^{n+m} = y^n \cdot y^m \in IJ$ , then  $y \in \sqrt{IJ}$ .

$y^{n+m} = y^n \cdot y^m \in I \cap J$ , then  $y \in \sqrt{I \cap J}$ . Thus  $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$

2). we have  $\sqrt{\sqrt{I}} \supseteq \sqrt{I}$  from Remark (1), we want to show that  $\sqrt{I} \supseteq \sqrt{\sqrt{I}}$ . Let  $x \in \sqrt{\sqrt{I}} \ni n \in \mathbb{Z}^+ \ni x^n \in \sqrt{I}$ , and then  $\exists m \in \mathbb{Z}^+ \ni (x^n)^m \in I$ , hence  $x^{nm} \in I$ , which implies that  $x \in \sqrt{I}$ . Thus  $\sqrt{I} \supseteq \sqrt{\sqrt{I}}$  and  $\sqrt{\sqrt{I}} = \sqrt{I}$

3). Let  $w \in \sqrt{I} + \sqrt{J}$ , then  $w = x + y$ ;  $x \in \sqrt{I}$  and  $y \in \sqrt{J}$ , then  $\exists n \in \mathbb{Z}^+ \ni x^n \in I$  and  $\exists m \in \mathbb{Z}^+ \ni y^m \in J$ .

$$(x + y)^{n+m} = x^{n+m} + \binom{n+m}{1} x^{n+m-1} y + \cdots + \binom{n+m}{n} x^n y^m + \binom{n+m}{n+1} x^{n-1} y^{m+1} + \cdots + y^{n+m}.$$

Thus  $(x + y)^{n+m} \in I + J$  then  $x + y \in \sqrt{I + J}$ .

### Definition:

A proper ideal  $I$  of a ring  $R$  is called **semiprime** if  $I = \sqrt{I}$ .

Example: In  $\mathbb{Z}$ ,  $\sqrt{6\mathbb{Z}} = 6\mathbb{Z}$ , so  $\langle 6 \rangle$  is semiprime ideal in  $\mathbb{Z}$ .

$\sqrt{\langle 4 \rangle} = \sqrt{\langle 2^2 \rangle} = \langle 2 \rangle$ , so  $\langle 4 \rangle$  is not semiprime ideal in  $\mathbb{Z}$

$\sqrt{10\mathbb{Z}} = 10\mathbb{Z}$ .

### Theorem:

Every prime ideal is semiprime.

**Proof:** Let  $I$  be a prime ideal,  $I \subseteq \sqrt{I}$  we have to show only that  $\sqrt{I} \subseteq I$ .

Let  $w \in \sqrt{I} \ni n \in \mathbb{Z}^+ \ni w^n \in I$ , then  $ww^{n-1} \in I$  but  $I$  be a prime ideal so either  $w \in I$  or  $w^{n-1} \in I$ .

If  $w^{n-1} \in I$ , then  $ww^{n-2} \in I$ , which implies that  $w^{n-2} \in I$  we continue in this way until we have  $w \in I$ .

**Remark:**

The converse is not true.

For example:  $\sqrt{\langle 6 \rangle} = \langle 6 \rangle$  is semiprime but it is not prime since  $2 \notin \langle 6 \rangle$ ,  $3 \notin \langle 6 \rangle$  but  $6 = 2 \cdot 3 \in \langle 6 \rangle$

**Theorem:**

A proper ideal  $I$  of a ring  $R$  is semiprime if and only if  $\frac{R}{I}$  has no nonzero nilpotent element.

**Proof:**  $\Rightarrow$ ) Let  $I$  be a semiprime ideal and let  $a + I$  be a nilpotent element in  $\frac{R}{I} \exists$  a positive integer such that  $(a + I)^n = I$ , hence  $a^n + I = I \Leftrightarrow a^n \in I \Rightarrow a \in \sqrt{I} = I$ . [ since  $I$  is semiprime ]. Thus  $a \in I \Leftrightarrow a + I = I$

$\Leftarrow$ ) we want to prove  $I$  is semiprime  $I \subseteq \sqrt{I}$  we have to show only that  $\sqrt{I} \subseteq I$ .

Let  $x \in \sqrt{I}$ , then  $x^n \in I \Leftrightarrow x^n + I = I$ , then  $(x + I)^n = I \Rightarrow x + I$  is a nilpotent element in  $\frac{R}{I}$ , hence  $x + I = I \Rightarrow x \in I$ . Thus  $\sqrt{I} \subseteq I$  and then  $\sqrt{I} = I$ .

**Definition:**

A proper ideal  $I$  of a ring  $R$  is called **primary** if whenever  $a \cdot b \in I$  and  $a \notin I$  implies that  $b^k \in I$  for some  $k \in \mathbb{Z}^+$ .

**Example:** In  $\mathbb{Z}$ . Let  $I = 8\mathbb{Z}$ ,  $4 \cdot 2 = 8 \in 8\mathbb{Z}$ ,  $4 \notin 8\mathbb{Z}$  and  $2^3 = 8 \in 8\mathbb{Z}$ , so  $8\mathbb{Z}$  is primary ideal.

**Remark:**

Every prime ideal is primary.

Q: Is the converse true?

$8\mathbb{Z}$  is primary ideal but not prime since  $4 \cdot 2 = 8 \in 8\mathbb{Z}$  but  $4 \notin 8\mathbb{Z}$  and  $2 \notin 8\mathbb{Z}$

**Theorem:**

Let  $R$  be a commutative ring with 1 and  $I$  be a proper ideal of  $R$ ,  $I$  is a primary ideal if and only if every zero divisor of  $\frac{R}{I}$  is nilpotent

**Proof:**  $\Rightarrow$ ) Let  $a + I$  be a zero divisor in  $\frac{R}{I}$ , so  $a + I \neq I$  and  $\exists b + I \neq I$  in  $\frac{R}{I}$  such that  $(a + I)(b + I) = I$ , then  $ba + I = I \Leftrightarrow ba \in I$  but  $b \notin I$  and  $I$  is primary, then  $\exists k \in \mathbb{Z}^+ \ni a^k \in I \Leftrightarrow a^k + I = I$  thus  $(a + I)^k = I$  and  $a + I$  is a nilpotent element.

$\Leftarrow$ ) Let  $x \cdot y \in I$  and  $x \notin I$ , then  $x \cdot y \in I \Leftrightarrow x \cdot y + I = I \Leftrightarrow (x + I)(y + I) = I$ , but  $x + I \neq I$

If  $y + I = I \rightarrow y \in I$ , we are done. [ $I$  is primary]

If  $y + I \neq I$ , then  $y + I$  is a zero divisor, hence by assumption  $y + I$  is a nilpotent element in  $\frac{R}{I} \ni \exists n \in \mathbb{Z}^+ \ni (y + I)^n = I = y^n + I = I \Leftrightarrow y^n \in I$ .

**Theorem:**

Let  $f : R \longrightarrow R'$  be a ring epimorphism.

1. If  $M$  is a maximal (prime, primary, semiprime) ideal in  $R$  with  $\ker f \subseteq M$ , then  $f(M)$  is maximal (prime, primary, semiprime) ideal in  $R'$ .
2. If  $M'$  is a maximal (prime, primary, semiprime) ideal in  $R'$ , then  $f^{-1}(M')$  is maximal (prime, primary, semiprime) ideal in  $R$ .

**Proof:**

1). Let  $f : R \longrightarrow R'$  be an epimorphism and let  $M$  be a maximal ideal in  $R$  contain  $\ker f$  we will prove that  $f(M)$  is maximal ideal in  $R'$ .

Clearly  $f(M)$  is an ideal in  $R'$

$f(M) \neq R'$  [If  $f(M) = R'$ , then  $1' \in f(M) \rightarrow 1' = f(m); m \in M$ . But  $f(1) = 1' \rightarrow f(m) = f(1) \rightarrow f(m-1) = 0 \rightarrow m-1 \in \ker f \subseteq M \rightarrow m - (m-1) \in M \rightarrow 1 \in M$  contradiction since  $M$  be a maximal,  $M \neq R$ ]

Let  $f(M) \subsetneq J \subseteq R'$ ,  $J$  is an ideal in  $R'$ , then  $\exists y \in J$  and  $y \notin f(M)$ .

But  $f$  is onto  $\rightarrow \exists x \in R \ni f(x) = y, x \notin M$ .

Then by theorem (let  $M$  be a proper ideal of a ring  $R$ . If  $M$  is maximal ideal in  $R$  iff  $\langle M, x \rangle = R, x \notin M$ )  $\langle M, x \rangle = R \rightarrow 1 = m + tx; m \in M, t \in R$ , then  $f(1) = f(m + tx)$ , then  $f(1) = f(m) + f(t)f(x)$  [ $f$  is homomorphism], then  $1' = f(m) + f(t)y$

$f(m) \in f(M) \subsetneq J$  and  $y \in f(M) \subsetneq J$ , hence  $1' \in J$ , which implies that  $J = R'$ . Thus  $f(M)$  is maximal in  $R'$ .

2). Let  $M'$  be a maximal ideal in  $R'$ , then clearly  $f^{-1}(M')$  is an ideal in  $R$ .  $f^{-1}(M') \neq R$ .

[If  $f^{-1}(M') = R$ , then  $f^{-1}(w) = 1; w \in M' \rightarrow f(1) \in M' \rightarrow 1' \in M'$ ]. Let  $f^{-1}(M') \subsetneq J \subseteq R$ , then

$\exists x \in J$  and  $x \notin f^{-1}(M')$  iff  $f(x) \notin M'; \langle M', f(x) \rangle = R'$ .

$w + r'f(x) = 1'; w \in M', r' \in R' \dots (*)$

Since  $f$  is onto, then  $\exists r \in R$  and  $k \in M$  s.t  $f(k) = w, f(1) = 1' f(r) = r'$ . Then  $(*)$  will be:  $f(k) + f(r)f(x) = f(1)$ , then  $f(k) + f(rx) = f(1)$  [ $f$  is homomorphism] and  $f(k + rx) = f(1)$ , then  $f(k + rx - 1) = 0$ , hence  $k + rx - 1 \in \ker f \subseteq f^{-1}(M') \subseteq J$  and  $f(k) = w$  then  $k \in f^{-1}(M') \subsetneq J$ ,

so  $k + rx \in J$ , then  $(k + rx) - (k + rx - 1) \in J$ , which implies that  $1 \in J$  and  $J = R$ . Thus  $f^{-1}(M)$  is maximal in  $R$ .

3) Let  $I$  be a prime ideal in  $R$ , clearly  $f(I)$  is an ideal in  $R'$

$f(I) \neq R'$  since if  $f(I) = R'$  and  $f$  is onto, then  $\exists x \in I$  s.t  $f(x) = 1'$ . But  $f(1) = 1' \rightarrow f(x) = f(1) \rightarrow f(x - 1) = 0 \rightarrow x - 1 \in \ker f \subseteq I$ , but  $x \in I$ , then  $x - (x - 1) \in I$  and  $1 \in I$  C!.

Now, let  $f(a)f(b) \in f(I)$ ;  $a, b \in R$ , since  $f$  is homo., then  $f(a.b) \in f(I)$ , then  $a.b \in I$ .

but  $I$  is prime ideal, so either  $a \in I$ , which implies that  $f(a) \in f(I)$  or  $b \in I$ , which implies that  $f(b) \in f(I)$ . Thus  $f(I)$  is a prime ideal in  $R'$ .

4). Let  $K$  be a prime ideal in  $R'$ , we have to show  $f^{-1}(K)$  is prime ideal in  $R$ . 1. Clearly  $f^{-1}(K)$  is an ideal in  $R$  since  $K$  be an ideal in  $R'$ .

2.  $f^{-1}(K) \neq R$ , if  $f^{-1}(K) = R \rightarrow 1 \in f^{-1}(K)$ , then  $1 = f^{-1}(w)$ ;  $w \in K \rightarrow f(1) \in K \rightarrow 1 \in K$  C! since  $K$  is proper ideal in  $R'$

3. Let  $x, y \in f^{-1}(K)$  and  $x \notin f^{-1}(M)$ , then  $f(x.y) \in K$ , since  $f$  is homomorphism, then  $f(x)f(y) \in K$  and  $f(x) \notin K$ , but  $K$  is a prime, so  $f(y) \in K \rightarrow y \in f^{-1}(K)$ . Thus  $f^{-1}(K)$  is prime.

5). If  $I$  is primary in  $R$ , we have to show that  $f(I)$  is primary in  $R'$ .

Let  $f(a).f(b) \in f(I)$  and suppose that  $f(a) \notin f(I)$ , we prove that  $(f(b))^n \in f(I)$ , for some  $n \in \mathbb{Z}^+$ .

$f(a.b) \in f(I)$  [ $f$  is homo.], hence  $a.b \in I, a \notin I$  since  $f(a) \notin f(I)$  and  $I$  is primary, then  $b^n \in I$  for some  $n \in \mathbb{Z}^+$ . Thus  $f(b^n) \in f(I) \rightarrow (f(b))^n \in f(I)$  and  $f(I)$  is primary in  $R'$ .

6) Suppose that  $K$  is primary ideal in  $R'$ , we prove that  $f^{-1}(K)$  is primary ideal in  $R$ .

$f^{-1}(K) \neq R$ , if  $f^{-1}(K) = R$  [ $1 \in f^{-1}(K) \Rightarrow f(1) \in K \Rightarrow 1_R \in K$  C!].

Let  $x.y \in f^{-1}(K)$  and  $x \notin f^{-1}(K)$

$f(x.y) \in K$  and  $f(x) \notin K$  then  $f(x).f(y) \in K$ , hence  $\exists n \in \mathbb{Z}^+ \ni (f(y))^n \in K$ , then  $f(y^n) \in K$ , then  $y^n \in f^{-1}(K)$ . Thus  $f^{-1}(K)$  is primary in  $R$ .

7) Suppose  $M$  is semiprime ideal in  $R$ .  $M = \sqrt{M}$ , we prove that  $f(M)$  is semiprime ideal in  $R'$ .

First,  $f(M) \neq R'$  [ $1_{R'} \in f(M) \rightarrow 1_{R'} = f(m), \exists n \in \mathbb{Z}^+$  such that  $f(m) = f(1)$ , then  $f(m-1) = 0$ , then  $(m-1) \in \text{Ker } f \subseteq M$ , then  $1 \in M$  C!].

We must show that  $f(M) = \sqrt{f(M)}$ , but we know that  $f(M) \subseteq \sqrt{f(M)}$ , so we only have to show  $\sqrt{f(M)} \subseteq f(M)$ . Let  $w \in \sqrt{f(M)}$ , then  $\exists n \in \mathbb{Z}^+ \ni w^n \in f(M)$ , then  $w^n = f(m); m \in M$ .

Since  $f$  is onto, then  $\exists x \in R \ni f(x) = w$ , then  $w^n = (f(x))^n = f(x^n) = f(m)$ , then  $(x^n - m) \in \text{Ker } f \subseteq M$ , then  $(x^n - m) \in M$  but  $m \in M$ , hence  $x^n \in M$ , then,  $x \in \sqrt{M} = M \Rightarrow x \in M$  [since  $M$  is semiprime and  $\sqrt{M} = M$ ], then  $f(x) \in f(M) \Rightarrow w \in f(M)$ , hence  $\sqrt{f(M)} \subseteq f(M)$ . Thus  $f(M) = \sqrt{f(M)}$  and  $f(M)$  is semiprime ideal in  $R'$ .

8) (H.W)

**Definition:**

The **Jacobson radical** of a ring  $R$ , denoted by  $J(R)$  is the set:

$$J(R) = \cap \{M : M \text{ is maximal ideal in } R\}$$

**Example:** (1) In  $\mathbb{Z}$ ,  $(2\mathbb{Z}) \cap (3\mathbb{Z}) \cap (7\mathbb{Z}) \cap \dots = \{0\}$ ,  $J(\mathbb{Z})=0$

(2) In  $\mathbb{Z}_6$ ,  $\{\bar{0}, \bar{2}, \bar{4}\} \cap \{\bar{0}, \bar{3}\} = \{0\}$ ,  $J(\mathbb{Z}_6)=0$ .

(3)  $\mathbb{Z}_4$ ,  $M = \{\bar{0}, \bar{2}\}$ .

$\therefore J(\mathbb{Z}_4) = \{\bar{0}, \bar{2}\}$ .

**Remark:**

1.  $J(R) \neq \emptyset$ .
2.  $J(R)$  is an ideal in  $R$ .

**Proof:** Let  $a, b \in J(R)$ , then  $a, b \in \cap \{M : M \text{ is maximal ideal in } R\}$ , then  $a, b \in M \forall \text{ maximal ideal } M$ , then  $a - b \in M \forall M$ , since  $M$  is an ideal in  $R$ ,  $a - b \in \cap M$ , hence  $a - b \in J(R)$ . Similarly  $ra \in J(R)$ .

**Theorem:**

Let  $I$  be an ideal in a ring  $R$ . Then  $I \subseteq J(R)$  if and only if the coset  $1 + I$  has invertible element in  $R$ .

**Proof:**  $\Rightarrow$ ) Let  $I \subseteq J(R)$  and assume that  $\exists a \in I$  such that  $1 + a$  has no inverse.  $\exists$  a maximal ideal  $M$  such that  $1 + a \in M$ ,  $a \in I \subseteq J(R) \subseteq M$ ,  $a \in M$ ,  $1 + a - a \in M \Rightarrow 1 \in M$

Hence  $M = R$ !. Thus  $1 + I$  has inverse.

$\Leftarrow$ ) suppose that each member of  $1 + I$  has inverse, but  $I \not\subseteq J(R) = \cap M$ ;  $M$  is maximal ideal, then  $I \not\subseteq M$ .

Now, if  $a \in I$ ,  $a \notin J(R)$ , then  $\exists$  a maximal ideal  $M$  s.t  $a \notin M$ . Since  $M$  is maximal, then  $\langle M, a \rangle = R$ , since  $1 \in R \Rightarrow 1 = m + ra$ ;  $r \in R, m \in M \Rightarrow m = 1 - ra$ , but  $1 - ra \in 1 + I$ , then  $m \in 1 + I$ , then  $m$  has inverse. Thus  $1 = mm^{-1} \in M$  C! [Since  $M = R$ ].

### Corollary:

$a \in J(R) \Leftrightarrow 1 + ra$  has inverse  $\forall r \in R$ .

**Proof:** Take  $I = \langle a \rangle$  by above lemma, we have  $a \in \langle a \rangle \subseteq J(R)$  if and only if  $1 + \langle a \rangle$  has inverse. Thus  $1 + ra$  has inverse.

### Lemma:

The uniqueness idempotent element in  $J(R)$  is 0.

**Proof:** Let  $a \in J(R)$ , such that  $a = a^2$ , then  $a - a^2 = 0$ , then  $a(1 - a) = 0$ ,  $a(1 + (-1)a) = 0 \cdots (*)$ . By the last corollary and since  $a \in J(R)$ , then  $1 + (-1)a$  has inverse, so  $\exists b \in R$  such that  $(1 + (-1)a)b = 1$  by (\*).

$a \cdot [(1 + (-1)a)b] = 0 \cdot b$ , so  $a \cdot 1 = 0$ . Thus  $a = 0$ .



**Definition:**

The ideal  $I$  is called nil ideal if each element in  $I$  is nilpotent.

**Example:**

In the ring  $Z_8$

The ideals are  $I_1 = \{\bar{0}, \bar{4}\}$ ,  $I_2 = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$  are nil ideals.

$I_1$  is a nil ideal since  $\bar{4}^2 = \bar{0}$ .

$I_2$  is a nil ideal since  $\bar{2}^3 = \bar{0}$ ,  $\bar{4}^2 = \bar{0}$ ,  $\bar{6}^3 = \bar{0}$

**Lemma:**

Every nil ideal contained in  $J(R)$ .

**Proof:** Let  $I$  be a nil ideal and we prove that  $I \subseteq J(R)$ . Let  $a \in I$ , since  $I$  is nil ideal, then  $\exists n \in \mathbb{Z}^+$  s.t  $a^n = 0$ , let  $r \in R$ . Now:

$$(1 + ra)(1 - ra + r^2a^2 - r^3a^3, \dots, (-1)^{n-1}(ra)^{n-1}) = 1 - r^n a^n = 1.$$

[Since  $a^n = 0$ , then  $r^n a^n = 0$  ]

By the last corollary  $a \in J(R)$ , then  $a \in I$ , which implies that  $I \subseteq J(R)$ .

**Lemma:**

$$J\left(\frac{R}{J(R)}\right) = 0.$$

**Proof:** Let  $J(R) = I$ , we prove that  $a + I = I$  i.e)  $1 + ra$  has inverse in  $R$ . Let  $a + I \in J\left(\frac{R}{J(R)}\right)$ , then  $(1 + I) + (r + I)(a + I)$  has inverse in  $\frac{R}{J(R)}$ , so  $\exists b + I \in$

$J\left(\frac{R}{J(R)}\right)$  such that  $[(1 + I) + (r + I)(a + I)](b + I) = 1 + I$ , then  $(1 + ra + I)(b + I) = 1 + I$ , then  $b(1 + ra) + I = 1 + I$ , then  $b(1 + ra) - 1 \in I$ , hence  $1 + r_1(b(1 + ra) - 1)$  has inverse. In special case take  $r_1 = 1$ , we have  $1 + (1)(b(1 + ra) - 1)$  has inverse in  $R$ , i.e)  $b(1 + ra)$  has inverse in  $R$ . Thus  $\exists w \in R$  s.t  $w.b(1 + ra) = 1$ , hence  $(1 + ra)$  has inverse, so that  $a \in J(R) = I$  and  $a + J(R) = J(R)$ .

**Definition:**

The **prime radical** of a ring  $R$ , denoted by  $L(R)$  is the set:

$$L(R) = \cap \{P : P \text{ is prime ideal in } R\}$$

**Example:**

- (1) In  $\mathbb{Z}$ :  $L(\mathbb{Z}) = \cap (P) = \{0\}$ ,  $L(\mathbb{Z}) = 0$ , where  $P$  is prime.
- (2) Find  $L(\mathbb{Z}_8)$ ,  $L(\mathbb{Z}_6)$ ,  $L(\mathbb{Z}_{12})$ . (H.W).
- (3) If  $R$  is an integral domain, then  $L(R) = 0$

**Remark:**

1.  $L(R) \neq \emptyset$ .
2.  $L(R)$  is an ideal in  $R$ .
3.  $L(R) \subseteq J(R)$

**Theorem(\*):**

Let  $I$  be a proper ideal in a ring  $R$ , then

$$\sqrt{I} = \cap \{P : P \text{ is prime ideal in } R \text{ contain } I\}$$

**Proof:**

1) Let  $r \notin \sqrt{I}$ , then  $r^n \notin I \forall n \in \mathbb{Z}$ , let  $S = \{r, r^2, r^3, \dots, r^n, \dots\}$ , then  $I \cap S = \emptyset$ , define  $F = \{J : J \cap S = \emptyset ; J \text{ is proper ideal contain } I\}$ ,  $F \neq \emptyset$  (since  $I \in F$ ), let  $\{C_\alpha\}_{\alpha \in \Lambda}$  be a chain of element from  $F$  i.e  $C_\alpha \cap S = \emptyset$ ,  $C_\alpha$  is a proper ideal contain  $I$ ,  $\forall \alpha$ , we will prove that  $\cup_{\alpha \in \Lambda} C_\alpha \in F$ , Let  $x, y \in \cup_{\alpha \in \Lambda} C_\alpha$ ,  $\exists \gamma, \beta \in \Lambda$  s.t  $x \in C_\beta$ ,  $y \in C_\gamma$ , since  $\{C_\alpha\}_{\alpha \in \Lambda}$  is a chain of  $F$ , then either  $x \in C_\beta \subseteq C_\gamma \ni y$  or  $x \in C_\gamma \subseteq C_\beta \ni x$ , then  $x, y \in C_\beta$  or  $x, y \in C_\gamma$ , then  $x - y \in C_\beta$  or  $x - y \in C_\gamma$ , hence  $x - y \in \cup_{\alpha \in \Lambda} C_\alpha$ .

Now, let  $r \in R$  and  $x \in \bigcup_{\alpha \in \Lambda} C_\alpha$ , then  $\exists \beta \in \Lambda$  s.t  $x \in C_\beta$ , then  $rx \in C_\beta$ . since  $\bigcup_{\alpha \in \Lambda} C_\alpha$  is an ideal in  $F$ .

2)  $\bigcup_{\alpha \in \Lambda} C_\alpha \neq R$  since if  $\bigcup_{\alpha \in \Lambda} C_\alpha = R$ , then  $1 \in \bigcup_{\alpha \in \Lambda} C_\alpha$ , hence  $\exists C_\gamma$  s.t  $1 \in C_\gamma$   $C_\gamma = R$ ! [since  $C_\alpha \forall \alpha$  is proper ideal of  $R$ ], since  $I \subseteq C_\alpha \forall \alpha$ . Thus  $I \subseteq \bigcup_{\alpha \in \Lambda} C_\alpha$ .

3)  $(\bigcup_{\alpha \in \Lambda} C_\alpha) \cap S = \bigcup_{\alpha \in \Lambda} (C_\alpha \cap S) = \bigcup (\emptyset) = \emptyset$ . Thus  $\bigcup_{\alpha \in \Lambda} C_\alpha \in F$ . By Zorn's Lemma  $F$  has a maximal element  $P$ .

Claim:  $P$  is prime  $P$  in  $R$ .

Suppose that  $P$  is not prime, let  $x, y \in P$  and  $x \notin P, y \notin P$ .

$$P \subsetneq \langle P, x \rangle$$

$$P \subsetneq \langle P, y \rangle$$

Since  $P$  is maximal in  $F$ , then  $\langle P, x \rangle, \langle P, y \rangle$  must intersect  $S$ .

i.e  $\langle P, x \rangle \cap S \neq \emptyset, \langle P, y \rangle \cap S \neq \emptyset$ .

Then  $\exists m, k \in \mathbb{Z}^+$  s.t  $r^m \in \langle P, x \rangle, r^k \in \langle P, y \rangle$ , then  $r^{m+k} = r^m \cdot r^k \in \langle P, x \rangle \cdot \langle P, y \rangle \subseteq \langle P, x, y \rangle = P$ .

Thus  $r^{m+k} \in P$  C! (since  $P \cap S = \emptyset$ ), then  $P$  is prime ideal and  $P \in F$ , hence  $\forall n \in \mathbb{Z}^+, r^n \notin P$  so  $r \notin P$ , then  $r \notin$  for any prime ideal contain  $I$ .

$r \notin \bigcap \{P : P \text{ is prime ideal contain } I\}$ , then  $\exists P ; P. \text{ is prime ideal contain } I$ . Thus  $r^n \notin P \forall n \in \mathbb{Z}^+$  [since  $P$  is prime ideal] i.e  $(r \cdot r = r^2 \notin P, r^2 \cdot r = r^3 \notin P, \dots)$  and  $r^n \notin I \forall n \in \mathbb{Z}^+, I \subseteq P$ .

If we put  $I = \{0\}$  we have:

Corollary:

$$\sqrt{\langle 0 \rangle} = \bigcap \{P : P \text{ is prime ideal in } R\} = L(R)$$

Since all prime ideals in  $R$  contain 0 we don't write  $0 \subseteq P$ .

- 1)  $L(R)$  = The set of all nilpotent element of  $R$ .
- 2)  $\sqrt{\langle 0 \rangle} = \{ r \in R : r^n = 0 \}$  The set of all nilpotent element.

**Theorem:**

An ideal  $I$  of a ring  $R$  is semiprime ideal iff  $I$  is an intersection of prime ideal of  $R$ .

**Example:**  $\sqrt{\langle 6 \rangle} = \langle 6 \rangle$

**Remark:**

$$L\left(\frac{R}{L(R)}\right) = 0.$$

**Proof:** Let  $x + L(R) \in L\left(\frac{R}{L(R)}\right)$ , then by ( )  $\exists n \in \mathbb{Z}$  s.t  $(x + L(R))^n = L(R)$ , then  $x^n + L(R) = L(R)$ , then  $x^n \in L(R)$ , then by ( )  $\exists n \in \mathbb{Z}$  s.t  $(x^n)^m = 0$ , hence  $x^{nm} = 0$ . Thus  $x \in L(R)$  iff  $x + L(R) = L(R)$ .

**Theorem:**

Let  $f : R \longrightarrow R'$  be an epimorphism such that  $\ker f \subseteq J(R)$ . Then:

1.  $f(J(R)) = J(R')$ .
2.  $f^{-1}(J(R')) = J(R)$ .

**Proof:**

1). Let  $f : R \longrightarrow R'$  be an epimorphism.

To prove that  $f(J(R)) = J(R')$  we must prove that  $f(J(R)) \subseteq J(R')$  and  $J(R') \subseteq f(J(R))$ .

Let  $w \in f(J(R))$ ,  $w = f(x)$ ;  $x \in J(R)$ . To prove  $w \in J(R')$  we have to show that  $1' + r'w$  has inverse where  $r' \in R'$ .

Since  $f$  is onto,  $\exists t \in R$  s.t  $f(t) = r'$  and  $f(1) = 1'$

$$1' + r'w = f(1) + f(t).f(x) = f(1 + tx) [f \text{ is homo.}]$$

Since  $x \in J(R)$ , then  $1 + kx$  has inverse in  $R$ ;  $k \in R$ .

In special case.  $1 + tx$  has inverse, i.e.  $\exists a \in R$  s.t  $(1 + tx).a = 1 \Rightarrow$

$$f(1 + tx).a = f(1) \Rightarrow [f(1) + f(t).f(x)].f(a) = f(1) [f \text{ is homo.}] \Rightarrow$$

$$(1' + r'w).f(a) = 1' \in R' \text{ i.e. } f(a) \text{ is an inverse to } 1' + r'w.$$

Hence  $w \in J(R')$  [theorem]. Thus  $f(J(R)) \subseteq J(R') \cdots (1)$ .

Now, to prove  $J(R') \subseteq f(J(R))$ .

Let  $y \in J(R')$ , since  $f$  is onto,  $\exists x \in R$  s.t  $f(x) = y$ , it is enough to show that  $x \in J(R)$  i.e.  $1 + rx$  has inverse.

Since  $y \in J(R') \Rightarrow 1' + r'y$  has inverse in  $R'$  [theorem].

$$\exists z \in R' \text{ s.t } z.(1' + r'y) = 1', 1' \in R', z \in R', r' \in R'.$$

Since  $f$  is onto,  $\exists r \in R$  s.t  $f(r) = r'$ ,  $\exists t \in R$  s.t  $f(t) = z$ ,  $f(1) = 1'$ .

$$(1' + r'y).z = 1' \Rightarrow [f(1) + f(r).f(x)].f(t) = f(1) \Rightarrow f((1 + rx).t) = f(1) \Rightarrow f((1 + rx).t - 1) = 0 \Rightarrow (1 + rx).t - 1 \in \ker f \subseteq J(R). \quad \text{Hence}$$

$1 + s[(1 + rx).t - 1]$  has an inverse  $\forall s \in R$ . In special case  $s = 1$ .

$1 + (1 + rx).t - 1$  has an inverse in  $R \Rightarrow (1 + rx).t$  has an inverse in  $R$ .

i.e.  $\exists w \in R$  s.t  $w.t(1 + rx) = 1$ , i.e.,  $1 + rx$  has an inverse  $(tw)$  in  $R$  iff  $x \in J(R)$ , hence  $J(R') \subseteq f(J(R)) \cdots (2)$ .

Thus from (1), (2)  $f(J(R)) = J(R')$

2) Now we want to show that  $f^{-1}(J(R')) = J(R)$ .

Let  $x \in f^{-1}(J(R')) \Rightarrow f(x) \in J(R') = f(J(R))$ , then  $f(x) \in f(J(R))$ , then  
 $\exists y \in J(R)$  s.t  $f(x) = f(y) \Rightarrow f(x - y) = 0 \Rightarrow x - y \in \ker f \subseteq J(R)$ ,  
 $x - y + y = x \in J(R)$  [since  $y, x - y \in J(R)$ ].

Hence  $f^{-1}(J(R')) \subseteq J(R) \dots (1)$ .

Now, let  $w \in J(R) \Rightarrow f(w) \in f(J(R)) = J(R') \Rightarrow f(w) \in J(R')$   
 $\Rightarrow w \in f^{-1}(J(R'))$ .

Hence  $J(R) \subseteq f^{-1}(J(R')) \dots (2)$ .

From (1), (2)  $\Rightarrow f^{-1}(J(R')) = J(R)$ .

### **Theorem:**

Let  $f : R \longrightarrow R'$  be an epimorphism such that  $\ker f \subseteq L(R)$ . Then:

1.  $f(L(R)) = L(R')$ .
2.  $f^{-1}(L(R')) = L(R)$ .

### **Proof:**

1). Let  $f : R \longrightarrow R'$  be an epimorphism.

To prove that  $f(L(R)) = L(R')$  we must prove that  $f(L(R)) \subseteq L(R')$  and  
 $L(R') \subseteq f(L(R))$ .

$$L(R) = \{x \in R : x^n = 0, \text{ for some } n \in \mathbb{Z}^+\} = \sqrt{\langle 0 \rangle}.$$

Let  $x \in f(L(R)) \Rightarrow \exists a \in L(R)$  s.t  $x = f(a) \Rightarrow a^n = 0, n \in \mathbb{Z}^+$ .

$$0' = f(0) = f(a^n) = (f(a))^n = x^n \Rightarrow x^n = 0' \Rightarrow x \in L(R').$$

Hence  $f(L(R)) \subseteq L(R')$ .

Let  $y \in L(R') \Rightarrow y^n = 0' \ n \in \mathbb{Z}^+$ , since  $f$  is onto  $\Rightarrow \exists b \in R$  s.t  $f(b) = y$ .

$0' = y^n = (f(b))^n = f(b^n)$ , since  $f$  is homo.  $\Rightarrow b^n \in \text{Ker } f \subseteq L(R)$

$\Rightarrow b^n \in L(R) \Rightarrow \exists m \in \mathbb{Z}^+$  s.t  $(b^n)^m = 0 \Rightarrow b^{mn} = 0 \Rightarrow b \in L(R)$ .

$y = f(b) \in f(L(R)) \Rightarrow L(R') \subseteq f(L(R))$ . Thus  $f(L(R)) = L(R')$ .

2) Now we want to show that  $f^{-1}(L(R')) = L(R)$ .

Let  $x \in f^{-1}(L(R')) \Rightarrow f(x) \in L(R') = f(L(R))$ , then  $f(x) \in f(L(R))$ , then

$\exists y \in L(R)$  s.t  $f(x) = f(y) \Rightarrow f(x - y) = 0$  [ $f$  is homo.]

$\Rightarrow x - y \in \text{ker } f \subseteq L(R)$ ,  $\Rightarrow x - y + y = x \in L(R)$  [since  $y, x - y \in L(R)$ ].

Hence  $f^{-1}(L(R')) \subseteq L(R) \dots (1)$ .

Now, let  $w \in L(R) \Rightarrow f(w) \in f(L(R)) = L(R') \Rightarrow f(w) \in L(R')$

$\Rightarrow w \in f^{-1}(L(R'))$ .

Hence  $L(R) \subseteq f^{-1}(L(R')) \dots (2)$ .

From (1), (2)  $\Rightarrow f^{-1}(L(R')) = L(R)$ .

### **Division Algorithm For Integral Domain:**

#### **Definition:**

Let  $R$  be a ring and let  $0 \neq a \in R, b \in R$  we say that “ $a$  divided  $b$ ” ( $a \mid b$ ) if

$\exists$  a number  $c$  s.t  $b = a.c$ .

#### **Remark:**

If  $a$  divided  $b$  we mean that  $a$  is a factor  $b$  or  $b$  multipolar  $a$ .



**Remark:**

$a \setminus b$  if and only if  $\langle b \rangle \subseteq \langle a \rangle$ .

**Proof:**  $\Rightarrow$ ) Suppose  $a \setminus b \Rightarrow b = a.c, c \in R, b \in \langle b \rangle \Rightarrow b \in \langle a \rangle \Rightarrow \langle b \rangle \subseteq \langle a \rangle$ .

$\Leftarrow$ ) Suppose  $\langle b \rangle \subseteq \langle a \rangle$  since  $b \in \langle b \rangle \Rightarrow b \in \langle a \rangle \Rightarrow b = a.r, r \in R$ .

Thus  $a/b$ .

**Theorem:**

Let  $R$  be a ring, then

- 1)  $1 \setminus a, a \setminus a, a \setminus 0 \quad \forall a \in R$ .
- 2)  $a \setminus 1$  iff  $a$  has inverse.
- 3) If  $a \setminus b, b \setminus c \Rightarrow a \setminus c$ .
- 4) If  $a \setminus b$ , then  $a.c \setminus b.c \quad \forall c \in R$ .
- 5)  $\forall a, b, c \in R$  if  $c \setminus a, c \setminus b$ , then  $c \setminus ax + by \quad \forall x, y \in R$ .

**Proof(1):**

Since  $a = 1.a \Rightarrow 1 \setminus a$  and since  $a = a.1 \Rightarrow a \setminus a$ .

$0 = a.0 \Rightarrow a \setminus 0$ .

**Proof(2):**

$\Rightarrow$ ) Since  $a \setminus 1 \Rightarrow 1 = a.b$  where  $b \in R$  which mean that  $b$  is an inverse of  $a$ .

$\Leftarrow$ )  $a$  has inverse  $\Rightarrow 1 = a.c, c \in R \Rightarrow a \setminus 1$ .

**Proof(3):**

Since  $a \setminus b, b \setminus c \Rightarrow \exists u_1, u_2 \in R$  s.t  $b = a.u_1, c = a.u_2$ .

$c = a.u_1.u_2 = a.(u_1.u_2)$ . Thus  $a \setminus c$ .

**Proof(4):**

Since  $a \setminus b \Rightarrow b = a.r, r \in R \Rightarrow c.b = c.a.r \Rightarrow c.a \setminus c.b$ .

**Proof(5):**

Since  $c \setminus a, c \setminus b \Rightarrow \exists r_1, r_2 \in R$  s.t  $a = c.r_1, b = c.r_2$ .

$a.x = c.r_1.x, by = c.r_2y$ .

$a.x + by = c.r_1.x + c.r_2y = c(r_1.x + r_2y)$ .

Thus  $c \setminus ax + by$ .

**Definition:**

Let  $R$  be a ring and let  $a, b \in R$ , we say that  $a, b$  are associated element if  $a = bu$ , where  $u$  is invertible element in  $R$ .

**Eexample:**

In  $\mathbb{Z}$ :  $2, -2$ .

$-2 = (-1).2$ .

$(-1)$  has an inverse in  $\mathbb{Z}$ .

**Remark(1):**

Define a relation  $\sim$  on  $R$  as follows:  $a \sim b$  iff  $a, b$  are associated elements, is an equivalent relation.

**Proof:**

- i.  $a \sim a \forall a \in R$ .
- ii. If  $a \sim b$  then  $b \sim a$ .  
 $a \sim b \Rightarrow a = bu, u$  is invertible element in  $R. \Rightarrow au^{-1} = b \Rightarrow b \sim a$ .
- iii. If  $a \sim b$  and  $b \sim c$  then  $a \sim c$ .  
 $a \sim b \Rightarrow a = bu_1; u_1$  is invertible element in  $R$ .  
 $b \sim c \Rightarrow b = cu_2; u_2$  is invertible element in  $R$ .  
 $a = cu_2 u_1 = c(u_2 u_1) \Rightarrow a \sim c$ . Thus  $\sim$  is an equivalent relation.

**Remark(2):**

Consider the Gaussian numbers denoted by  $Z(i)$ .

$$Z(i) = \{a + ib : a, b \in \mathbb{Z}, i^2 = -1\} \subseteq \mathbb{C}$$

1.  $(Z(i), +, \cdot)$  is a ring but not field.?
2.  $Z(i)$  is an integral domain?

Here the only invertible elements are  $\pm 1, \pm i$ . Suppose  $a + ib \in Z(i)$  has a multiplicative inverse  $c + id$ . Then

$$(a + ib) \cdot (c + id) = 1, \text{ so } (a - ib) \cdot (c - id) = 1, \text{ then}$$

$$(a + ib) \cdot (c + id) \cdot (a - ib) \cdot (c - id) = 1$$

$$(a^2 + b^2)(c^2 + d^2) = 1, \quad a, b, c, d \in \mathbb{Z}$$

$$\Rightarrow (a^2 + b^2) = 1, \quad a^2 = 0, \quad b^2 = 1 \Rightarrow a = 0, \quad b = \pm 1.$$

Or  $a^2 = 1, \quad b^2 = 0 \Rightarrow a = \pm 1, \quad b = 0$ . Thus the invertible elements are  $\pm 1, \pm i$ .

The only associated elements of  $a + ib$  are:

$$a + ib, -a - ib, -b + ia, -b - ia.$$

**Theorem:**

Let  $a, b$  be a non-zero element of a ring  $R$ . Then the following statements are equivalent:

- 1)  $a, b$  are associates.
- 2) Both  $a \mid b$  and  $b \mid a$ .
- 3)  $\langle a \rangle = \langle b \rangle$ .

**Proof:**

1) $\Rightarrow$ 2) Suppose that  $a, b$  are associated elements  $\Rightarrow \exists$  an invertible element  $u \in R$  s.t  $a = bu \Rightarrow b \setminus a \Rightarrow u^{-1}a = b \Rightarrow a \setminus b$ .

2) $\Rightarrow$ 3)  $\because a \setminus b \Rightarrow \langle b \rangle \subseteq \langle a \rangle$ .

$\because b \setminus a \Rightarrow \langle a \rangle \subseteq \langle b \rangle$ .

$\Rightarrow \langle a \rangle = \langle b \rangle$ .

3) $\Rightarrow$ 2)  $\because \langle a \rangle = \langle b \rangle \Rightarrow \langle a \rangle \subseteq \langle b \rangle$  iff  $b \setminus a$  and  $\langle b \rangle \subseteq \langle a \rangle$  iff  $a \setminus b$

2) $\Rightarrow$ 1)  $\because a \setminus b \Rightarrow b = u_1 a \Rightarrow u_1 = ba^{-1}$  and  $\because b \setminus a \Rightarrow a = u_2 b \Rightarrow u_2 = ab^{-1}$ .

$u_1 u_2 = ba^{-1}ab^{-1} = bb^{-1} = 1 \Rightarrow u_1, u_2$  are invertible element.  $\Rightarrow a, b$  are associated elements

**Definition:**

Let  $a_1, a_2, \dots, a_n$  be a non-zero element of a ring  $R$ . An element  $d \in R$  is a greatest common divisor of  $a_1, a_2, \dots, a_n$  if satisfy the following:

- 1)  $d \mid a_i \quad \forall i = 1, 2, \dots, n$  .
- 2) If  $c \mid a_i \quad \forall i = 1, 2, \dots, n$  implies that  $c \mid d$  .

$$d = g.c.d(a_1, a_2, \dots, a_n).$$

**Example:**

$$g.c.d(30, 40) = 10.$$

**Theorem:**

Let  $a_1, a_2, \dots, a_n$  be a non-zero element of a ring  $R$ , then  $a_1, a_2, \dots, a_n$  have  $g.c.d$  of the form  $d = r_1a_1 + r_2a_2 + \dots + r_na_n$   $\iff$  the ideal  $\langle a_1, a_2, \dots, a_n \rangle$  is principal.

**Proof:**  $\Rightarrow$ 

Suppose that  $d = r_1a_1 + r_2a_2 + \dots + r_na_n \Rightarrow d \in \langle a_1, a_2, \dots, a_n \rangle$

$$\Rightarrow \langle d \rangle \subseteq \langle a_1, a_2, \dots, a_n \rangle.$$

Now, let  $x \in \langle a_1, a_2, \dots, a_n \rangle$ .

$$\Rightarrow x = t_1a_1 + t_2a_2 + \dots + t_na_n \quad ; \quad t_i \in R \quad \dots (*)$$

But  $d \mid a_i \quad \forall i = 1, 2, \dots, n \Rightarrow a_i = ds_i \quad ; \quad s_i \in R \quad \forall i = 1, 2, \dots, n$  .

Put  $a_i$  in  $(*)$ .

$$\Rightarrow x = t_1ds_1 + t_2ds_2 + \dots + t_nds_n = d(t_1s_1 + t_2s_2 + \dots + t_ns_n) = d.w.$$

$\therefore x \in \langle d \rangle \Rightarrow \langle a_1, a_2, \dots, a_n \rangle = \langle d \rangle$ . Thus is principal.

$\Leftarrow$ ) Now, suppose that  $\langle d \rangle = \langle a_1, a_2, \dots, a_n \rangle$ . To show that  $d$  is a greatest common divisor of  $a_1, a_2, \dots, a_n$ .

$a_i \in \langle d \rangle \forall i = 1, 2, \dots, n \Rightarrow \exists b_i \in R \text{ s.t. } a_i = db_i \Rightarrow d \mid a_i \forall i = 1, 2, \dots, n$ . Now, suppose that  $\exists c \in R \text{ s.t. } c \mid a_i \forall i \Rightarrow \exists s_i \in R \text{ s.t. } a_i = s_i c \Rightarrow$

$$\begin{aligned} d &= r_1 a_1 + r_2 a_2 + \dots + r_n a_n \\ &= r_1 s_1 c + r_2 s_2 c + \dots + r_n s_n c \\ d &= (r_1 s_1 + r_2 s_2 + \dots + r_n s_n) \cdot c \Rightarrow c \mid d \\ \therefore d &\text{ is g.c.d.}(a_1, a_2, \dots, a_n) \end{aligned}$$

### Corollary:

Any finite set of non-zero elements  $a_1, a_2, \dots, a_n$  of  $P.I.D$  has  $g.c.d.$

In fact  $g.c.d(a_1, a_2, \dots, a_n) = r_1 a_1 + r_2 a_2 + \dots + r_n a_n$  for suitable choice  $r_1, r_2, \dots, r_n \in R$ .

### Definition:

Let  $R$  be a ring and let  $a_1, a_2, \dots, a_n$  be a non-zero element of  $R$ . If  $R = \langle d \rangle = \langle a_1, a_2, \dots, a_n \rangle$ , then  $g.c.d(a_1, a_2, \dots, a_n) = 1$  and  $a_1, a_2, \dots, a_n$  are called relatively prime elements.

### Theorem:

Let  $a, b, c$  be elements of a  $P.I.D R$ , if  $c \mid ab$  with  $a, c$  relatively prime, then  $c \mid b$ .

### Proof:

Since  $a, c$  are relatively prime elements

$$\Rightarrow g.c.d(a, c) = 1 \Rightarrow 1 = ra + sc \quad ; \quad r, s \in R$$

Since  $c \setminus ab \Rightarrow ab = tc$  ;  $t \in R \Rightarrow b = bra + bsc$

$b = rtc + bsc = (rt + bs)c$  . Thus  $c \setminus b$ .

### Definition:

Let  $R$  be a ring and let  $a_1, a_2, \dots, a_n$  be non-zero elements of  $R$  , then  $d \in R$  is a least common multiple of  $a_1, a_2, \dots, a_n$  if  $a_i \setminus d \ \forall i = 1, 2, \dots, n$ . If  $\exists c \in R$  s.t  $a_i \setminus c$  , then  $d \setminus c$

$$d = l.c.m(a_1, a_2, \dots, a_n).$$

### Theorem:

Let  $a_1, a_2, \dots, a_n$  be a non-zero element of  $R$ , then  $a_1, a_2, \dots, a_n$  have least common multiple iff the ideal  $\cap \langle a_i \rangle$  is principale

### Proof: $\Rightarrow$

Let  $c = l.c.m(a_1, a_2, \dots, a_n)$ , we must prove that  $\cap \langle a_i \rangle = \langle c \rangle$ . Let  $w \in \langle c \rangle \Rightarrow w = rc$  ;  $r \in R$

But  $c$  is  $l.c.m(a_1, a_2, \dots, a_n) \Rightarrow a_i \setminus c \ \forall i = 1, 2, \dots, n$

$$\Rightarrow c = t_i a_i \ ; \ t_i \in R \ \forall i = 1, 2, \dots, n$$

$$w = rt_i a_i \ \forall i = 1, 2, \dots, n \Rightarrow w = rt_1 a_1 \Rightarrow w \in \langle a_1 \rangle.$$

$$, \ w = rt_2 a_2 \Rightarrow w \in \langle a_2 \rangle , \dots, \ w = rt_n a_n \Rightarrow w \in \langle a_n \rangle.$$

$$w \in \langle a_i \rangle \forall i \Rightarrow w \in \cap \langle a_i \rangle \Rightarrow \langle c \rangle \subseteq \cap \langle a_i \rangle.$$

Let  $k \in \cap_{i=1}^n \langle a_i \rangle \Rightarrow k \in \langle a_i \rangle \forall i \Rightarrow k = s_i a_i \ ; \ s_i \in R \ \forall i = 1, 2, \dots, n.$

$$\Rightarrow a_i \setminus k \ \forall i \text{ but } c = l.c.m(a_1, a_2, \dots, a_n),$$

$$\therefore c \setminus k \Rightarrow k = rc \ ; \ r \in R \Rightarrow k \in \langle c \rangle.$$

$$\cap_{i=1}^n \langle a_i \rangle \subseteq \langle c \rangle , \therefore \langle c \rangle = \cap_{i=1}^n \langle a_i \rangle.$$

$\Leftarrow$ ) Let  $\langle c \rangle = \cap_{i=1}^n \langle a_i \rangle$ , we prove that  $c = l.c.m(a_1, a_2, \dots, a_n)$ .

$$c \in \langle c \rangle \Rightarrow c \in \cap_{i=1}^n \langle a_i \rangle \Rightarrow c \in \langle a_i \rangle \forall i \Rightarrow c = t_i a_i \forall i \quad t_i \in R .$$

$$\Rightarrow a_i \mid c \quad \dots (1) .$$

We suppose that  $\exists c' \in R$  s.t  $a_i \mid c' \quad \forall i$ , we must prove that  $c \mid c'$ .

$$a_i \mid c' \Rightarrow c' = r_i a_i \forall i \quad r_i \in R \Rightarrow c' \in \langle a_i \rangle \forall i .$$

$$\Rightarrow c' \in \cap_{i=1}^n \langle a_i \rangle \Rightarrow c' \in \langle c \rangle .$$

$$c' = w.c \Rightarrow c \mid c' \quad \dots (2) .$$

From (1), (2)  $\Rightarrow c$  is  $l.c.m(a_1, a_2, \dots, a_n)$ .

### Corollary:

If  $R$  is  $P.I.D$ , then every finite set of non-zero elements have  $l.c.m..$

### Proof:

Let  $a_1, a_2, \dots, a_n$  be non-zero elements, then  $\cap_{i=1}^n \langle a_i \rangle$  is an ideal

$\exists c \in R$  s.t  $\langle c \rangle = \cap_{i=1}^n \langle a_i \rangle$  since  $R$  is  $P.I.D$ . Thus by the last theorem

$$c = l.c.m(a_1, a_2, \dots, a_n) .$$

### Definition:

Let  $R$  be a ring with 1. The element  $a \in R$  is called prime element if  $a \neq 0$ ,  $a$  has no inverse and  $a \mid c.b$ , then either  $a \mid c$  or  $a \mid b$ .

### Definition:

Let  $R$  be a ring with 1, then the element  $b \in R$  is called irreducible element if  $b \neq 0$ ,  $b$  has no inverse and if  $b = a.c$ , then either  $a$  has an inverse or  $c$  has an inverse.

### Theorem:



- 1) If  $p$  is prime element in  $R$  and  $p'$  is associated with  $p$ , then  $p'$  is prime element.
- 2) If  $q$  is irreducible element in  $R$  and  $q, q'$  are associated, then  $q'$  is irreducible element.

**Proof:**

- 1) Since  $p, p'$  are associated, then  $p' = up$  where  $u$  has an inverse.
  - a)  $p' \neq 0$  since if  $p' = 0 \Rightarrow 0 = up \Rightarrow p = 0$  C! [since  $p$  is prime element].
  - b)  $p'$  has no inverse since if  $p'$  has an inverse.
 
$$(p')^{-1} \cdot p' = (p')^{-1} \cdot up \Rightarrow 1 = [(p')^{-1} \cdot u] \cdot p \Rightarrow p \text{ is invertible C!}$$
 [since  $p$  is prime element].
  - c) If  $p' \nmid c \cdot b \Rightarrow c \cdot b = t \cdot p'$ ,  $t \in R \Rightarrow c \cdot b = t \cdot u \cdot p \Rightarrow c \cdot b = (t \cdot u) \cdot p \Rightarrow p \mid c \cdot b$  but  $p$  is prime element, then either  $p \mid c$  or  $p \mid b$  if  $p \mid b \Rightarrow b = r \cdot p \Rightarrow b = (r \cdot u) \cdot p' \Rightarrow p' \mid b$ . Similarly, if  $p \mid c \Rightarrow p'$  is prime element.
- 2) Since  $q, q'$  are associated, then  $q' = uq$  where  $u$  has an inverse  $\Rightarrow u^{-1} \cdot q' = q \dots (*)$ .
  - a)  $q' \neq 0$  since if  $q' = 0 \Rightarrow 0 = uq \Rightarrow q = 0$  C! [since  $q$  is prime element].
  - b)  $q'$  has no inverse since if  $q'$  has inverse  $\Rightarrow (q')^{-1} \cdot q' = (q')^{-1} \cdot uq \Rightarrow 1 = [(q')^{-1} \cdot u] \cdot q \Rightarrow q$  has inverse C! [since  $q$  is prime element].
  - c) If  $q' = c \cdot b \Rightarrow u \cdot q = c \cdot b \Rightarrow q = (u^{-1} \cdot b) \cdot c$  since  $q$  is irreducible element, then either  $c$  has an inverse or  $u^{-1} \cdot b$  has an inverse. If  $u^{-1} \cdot b$  has an inverse  $\Rightarrow \exists w \in R$  s.t.  $w(u^{-1} \cdot b) = 1$ 

$$\Rightarrow (wu^{-1})b = 1$$

$$\Rightarrow b \text{ has an inverse. Thus } q' \text{ is irreducible element.}$$

**Theorem:**

Let  $R$  be an I.D, then every prime element in  $R$  is irreducible element.

**Proof:**

Let  $p$  be a prime element in  $R$  and let  $a, b \in R$  s.t  $p = a.b$  (1.  $p = a.b$ )  $\Rightarrow p \nmid a.b$ ,  $p$  is prime element, then either  $p \nmid a$  or  $p \nmid b$ . if  $p \nmid a \Rightarrow a = r.p, r \in R \Rightarrow a.b = (r.p).b \Rightarrow p = r.b.p \Rightarrow 1 = r.b \Rightarrow b$  has an inverse.

Similarly if  $p \nmid b \Rightarrow p$  is irreducible element.

**Note**

The converse is not true?

**Theorem:**

Let  $R$  be a P I.D and let  $p \in R$ , then  $p$  is prime element iff  $p$  is irreducible element.

**Proof:**  $\Rightarrow$ )

From the last theorem

$\Leftarrow$ )

Let  $p \in R$  be an irreducible element and suppose that  $p \nmid a.b \Rightarrow p = a.b$  ;  $c \in R \cdots (*)$ .

$R$  is P I. D, then  $\langle a, p \rangle$  is principle

$\therefore \exists d \in R$  s.t  $\langle a, p \rangle = \langle d \rangle. \Rightarrow p = k.d$  ,  $k \in R$  but  $p$  is irreducible element  $\Rightarrow k$  has an inverse or  $d$  has an inverse.

If  $k$  has an inverse  $\Rightarrow d = k^{-1}p \Rightarrow d \in \langle d \rangle \Rightarrow \langle d \rangle \subseteq \langle p \rangle$  but  $a \in \langle d \rangle \Rightarrow a \in \langle p \rangle \Rightarrow a = r.p$  ;  $r \in R \Rightarrow p \nmid a$ .

If  $d$  has an inverse  $\Rightarrow 1 = dd^{-1} \in \langle d \rangle \Rightarrow \langle d \rangle = R$  but  $\langle d \rangle = \langle a, p \rangle \Rightarrow \langle a, p \rangle = R$ .

$$1 \in R = \langle a, p \rangle \Rightarrow 1 = at_1 + pt_2 \quad ; \quad t_1, t_2 \in R$$

$$b = bat_1 + bpt_2$$

$$b = bct_1 + pbt_2$$

$$b = p(ct_1 + bt_2)$$

$$\Rightarrow p \mid b.$$

$$16 \quad , \quad \text{contf}(x) = g.c.d(4, -32, -16) = 4$$

Corollary:

In  $Z$  there is no difference between irreducible element and prime element.

Proof:(H.W)

Remark:

Let  $R$  be a P.I.D. If  $\{I_n\}$  ;  $n \in \mathbb{Z}^+$  is any infinite sequence of ideals of  $R$  s.t  $I_1 \subseteq I_2 \subseteq \dots \subseteq I_n \subseteq I_{n+1} \subseteq \dots$  , then there exist  $m \in \mathbb{Z}^+$  s.t  $I_n = I_m$  for all  $n > m$ .

Proof:

Let  $\bigcup_{k=1}^{\infty} I_k = I$  , and  $I_1 \subseteq I_2 \subseteq \dots$  is a chain.

$\bigcup_{k=1}^{\infty} I_k$  is an ideal?

$R$  is P.I.D, then  $\exists a \in R$  s.t  $I = \langle a \rangle \Rightarrow a \in \bigcup_{k=1}^{\infty} I_k \Rightarrow \exists m \in \mathbb{Z}^+$  s.t  $a \in I_m$  for all  $n > m \Rightarrow I = \langle a \rangle \subseteq I_m \subseteq I_n \subseteq \bigcup_{k=1}^{\infty} I_k = I$  .  
 $\therefore I_m = \bigcup_{k=1}^{\infty} I_k$ . Thus  $I_n = I_m$ .

Definition:

The principle ideal is called maximal principle ideal if it's maximal in the set of proper principle ideals of  $R$  .

Theorem:

Let  $R$  be an integral domain for non-zero element  $p \in R$ , the following holds:

1.  $P$  is irreducible element iff  $\langle p \rangle$  is maximal principle ideal.
2.  $P$  is prime element iff  $\langle p \rangle \neq R$  is prime ideal.

Proof:1)  $\Rightarrow$

Let  $P$  be irreducible element, and let  $\langle p \rangle \subseteq \langle a \rangle$  ,  $a \in R$  .

$$p \in \langle p \rangle \Rightarrow p \in \langle a \rangle, \quad p = a.c, \quad c \in R \quad \dots (*)$$

But  $P$  is irreducible element  $\Rightarrow$  either  $a$  or  $c$  has an inverse. If  $c$  has an inverse  $\Rightarrow c^{-1}p = a$  [by  $(*)$ ]  $\Rightarrow a \in \langle p \rangle \Rightarrow \langle a \rangle \subseteq \langle p \rangle$   $C!$ , hence  $a$  has an inverse  $\Rightarrow a.a^{-1} = 1 \in \langle a \rangle \Rightarrow \langle a \rangle = R$ . Thus  $\langle p \rangle$  is maximal principle ideal.

$\Leftarrow$ )

Let  $\langle p \rangle$  be a maximal principle ideal.

Let  $p = a.b$ , suppose that  $a, b$  has no inverse  $p \in \langle a \rangle \Rightarrow \langle p \rangle \subset \langle a \rangle$  if  $a \in \langle p \rangle \Rightarrow a = p.c, \quad c \in R$ .

$a.b = p.c.b \Rightarrow p = p.c.b$  [ $R$  is I.D]  $\Rightarrow c.b = 1 \Rightarrow b$  has an inverse  $C! \therefore \langle p \rangle \subseteq \langle a \rangle$ .

Next if  $\langle a \rangle = R \Rightarrow a$  has inverse

$$\therefore \langle a \rangle \neq R \quad C! \text{ [since } a \text{ has no inverse]} \Rightarrow \langle p \rangle \subsetneq \langle a \rangle \subset R$$

Since  $\langle p \rangle$  is maximal principle ideal  $\therefore a$  or  $b$  has an inverse.

$\therefore P$  is irreducible element.

2)  $\Rightarrow$ )

Let  $P$  be prime element,  $\langle p \rangle \neq R$  [ $\text{since } p \text{ has no inverse}$ ]

Let  $a.b \in \langle p \rangle \Rightarrow a.b = k.p, \quad k \in R \Rightarrow p \nmid a.b$  but  $P$  is prime element  $\Rightarrow$  either  $p \nmid a$  or  $p \nmid b$

If  $p \nmid a \Rightarrow a = pk_1, \quad k_1 \in R \Rightarrow a \in \langle p \rangle$

Or  $p \nmid b \Rightarrow b = pk_2, \quad k_2 \in R \Rightarrow b \in \langle p \rangle$

$\therefore \langle p \rangle$  is prime ideal.

$\Leftarrow$ )

Suppose that  $\langle p \rangle$  is prime ideal  $\therefore \langle p \rangle \neq R \Rightarrow p$  has no inverse.

Let  $p \nmid a.b \Rightarrow a.b = m.p$  ,  $m \in R \Rightarrow a.b \in \langle p \rangle$  but  $P$  is prime element  
 $\Rightarrow$  either  $a \in \langle p \rangle \Rightarrow a = k_1 p$  ,  $k_1 \in R$

Or  $b \in \langle p \rangle \Rightarrow b = k_2 p$  ,  $k_2 \in R$  .

$\Rightarrow$  Either  $p \nmid a$  or  $p \nmid b$

Lemma: (\*)

Let  $R$  be a P.I.D,  $0 \neq a \in R$  .  $a$  has no inverse, then there exists a prime element  $p$  s.t  $p \nmid a$ .

Proof:

$\because a$  has no inverse  $\Rightarrow \langle a \rangle \neq R \Rightarrow \langle a \rangle$  is proper ideal of  $R$  .  $\Rightarrow \exists$  a maximal ideal  $M$  s.t  $\langle a \rangle \subset M$  .

$\because R$  is P.I.D  $\Rightarrow \exists p \in R$  s.t  $M = \langle p \rangle$   $\therefore \langle a \rangle \subset \langle p \rangle$ , then  $\langle p \rangle$  is maximal principle ideal.

But every maximal ideal is prime ideal, where  $p$  is prime element [by last Thm.(2) .

$a \in \langle a \rangle \subset \langle p \rangle \Rightarrow a \in \langle p \rangle \Rightarrow a = m.p$  ,  $m \in R \Rightarrow p \nmid a$ .

Definition:

An integral domain  $R$  is unique factorization domain (UFD) if the following are satisfied:

- (1)  $\forall a \in R$  s.t  $a \neq 0$  and has no inverse, then  $a = p_1.p_2 \dots p_n$  where  $p_i$  are irreducible elements  $\forall i$  .
- (2) If  $a = p_1.p_2 \dots p_n = q_1.q_2 \dots q_m$  where  $p_i, q_i$  are irreducible element  $\forall i$ , then  $n = m$  and there is a permutation  $\pi$  on  $\{1, 2, \dots, n\}$  s.t  $p_i, q_j$  are associated elements.

Example:

$\mathbb{Z}$  is UFD.

$$24 = (2) \cdot (2) \cdot (3) \cdot (2) = (-2) \cdot (-3) \cdot (2) \cdot (2).$$

Notice that  $2, -2$  are associated and  $3, -3$  are associated.

### Theorem:

Every PID is UFD.

### Proof:

Let  $R$  be a P I.D, and let  $0 \neq a \in R$  be an element which has no invers. Then  $a = p_1 \cdot p_2 \dots p_n$  by theorem ()  $p_i$  is irreducible elements  $\forall i$ . Now suppose that  $a = p_1 \cdot p_2 \dots p_n = q_1 \cdot q_2 \dots q_m$

Now we must show that  $n = m$ .

Suppose that  $n < m$ .

Notice that  $p_1 \nmid a \Rightarrow p_1 \nmid (q_1 \cdot q_2 \dots q_m)$ , but  $p_1$  is prime element  $\Rightarrow p_1 \nmid q_j$  for some  $j$ , after arranging.

$p_1$  and  $q_1$  are prime element in  $R$  and

$p_1 \nmid q_1 \Rightarrow q_1 = u p_1$  where  $u$  is an invertible element in  $R$ .

$$p_1 \cdot p_2 \dots p_n = u \cdot p_1 \cdot q_2 \dots q_m \Rightarrow p_2 \dots p_n = u \cdot q_2 \dots q_m.$$

We continue with these steps to  $(n - 1)$  times

$\Rightarrow 1 = (u_1 \cdot u_2 \dots u_n) \cdot q_{n+1} \dots q_m \Rightarrow q_{n+1}, \dots, q_m$  has an inverse in  $R$ .

$$\therefore n = m$$

$$q_1 \cdot q_2 \dots q_m = p_1 \cdot p_2 \dots p_n \Rightarrow q_j = 1 \cdot p_i$$

$q_j, p_i$  are associated for every  $i$ .

### Theorem:

Let  $R$  be a UFD if  $p$  is an irreducible element, then  $p$  is prime element.

### Proof:

Let  $p$  be an irreducible element and suppose that

$$p \mid a \cdot b \Rightarrow a \cdot b = c \cdot p \quad \dots (1)$$

1) If  $b$  has inverse

$$\Rightarrow a \cdot b \cdot b^{-1} = c \cdot b^{-1} \cdot p \Rightarrow a = (c \cdot b^{-1}) \cdot p \Rightarrow p \mid a.$$

2) If  $a$  has inverse

$$\Rightarrow a^{-1} \cdot a \cdot b = a^{-1} \cdot c \cdot p \Rightarrow b = (a^{-1} \cdot c) \cdot p \Rightarrow p \mid b. \therefore p \text{ is prime}$$

3) If  $c$  has inverse

$$\Rightarrow a \cdot b \cdot c^{-1} = c \cdot c^{-1} \cdot p \Rightarrow (a \cdot b) \cdot c^{-1} = p \Rightarrow a \cdot b \mid p \quad C! \\ (\text{since } p \nmid a \cdot b)$$

4) If  $a, b, c$  have no inverse

$$R \text{ is UFD} \Rightarrow a = p_1 \cdot p_2 \dots p_n, \quad b = q_1 \cdot q_2 \dots q_m, \quad c = k_1 \cdot k_2 \dots k_r.$$

Where  $p_i, q_j, k_l$  are irreducible elements

$$i = 1, 2, \dots, n, \quad j = 1, 2, \dots, m, \quad l = 1, 2, \dots, r.$$

Subdud in (1).

$$(p_1 \cdot p_2 \dots p_n) \cdot (q_1 \cdot q_2 \dots q_m) = (k_1 \cdot k_2 \dots k_r) \cdot p.$$

$P$  is associated with  $p_i(i.e)p_i = w \cdot p$ ,  $w$  has an inverse.

Or  $P$  is associated with  $q_j(i.e)q_j = u \cdot p$ ,  $u$  has an inverse.

$$\therefore a = p_1 \cdot p_2 \dots p_i \cdot p_{i+1} \dots p_n.$$

$$= p_1 \cdot p_2 \dots (w \cdot p) \cdot p_{i+1} \dots p_n = p \cdot (p_1 \cdot p_2 \dots w \cdot p_{i+1} \dots p_n).$$

$$\Rightarrow p \mid a$$

$$\therefore b = q_1 \cdot q_2 \dots q_j \cdot q_{j+1} \dots q_m.$$

$$= q_1 \cdot q_2 \dots (u \cdot p) \cdot q_{j+1} \dots q_m = p \cdot (q_1 \cdot q_2 \dots u \cdot q_{j+1} \dots q_m).$$

$$\Rightarrow p \mid b$$



$\Rightarrow p$  is prime number.

### Rings of polynomials Definition:

Let  $R$  be a ring, then the function  $f: \mathbb{Z}^+ \cup \{0\} \rightarrow R$  is called infinite sequence in  $R$  and we shall denote to  $f(n)$  by  $r_n$ ,  $\forall n \in \mathbb{Z}^+ \cup \{0\}$ .

$r_n$  is called the  $n$ th term (or general term) for the sequence  $\langle r_n \rangle$ .

$$f(n) = (r_0, r_1, \dots, r_n, \dots)$$

### Definition:

Let  $R$  be a ring, every infinite sequence in  $R$  (all terms equal zero except a finite of terms) is called a polynomial ring in  $R$  i.e.  $\exists$  a positive integer  $n$  such that  $r_m = 0 \forall m \geq n$ .

### Examples:

- (1)  $(0, 0, \dots, 0, \dots)$
- (2)  $(5, 4, -1, 0, 3, 0, 0, \dots)$
- (3)  $(0, 0, 0, -1, 2, 4, 0, 0, \dots)$

Are polynomial rings in  $R$ .

### Remark:

We will denote to all polynomial rings in  $R$  by  $R[x]$

$$R[x] = \{(a_1, a_2, a_3, \dots, a_n, 0, 0, \dots) : a_i \in R\}$$

### Remark:

Let  $\alpha = (a_1, a_2, a_3, \dots, a_n, 0, \dots)$  and  $\beta = (b_1, b_2, b_3, \dots, b_n, 0, \dots)$   $\alpha, \beta \in R[x]$ , then  $\alpha = \beta$  iff  $a_i = b_i \forall i = 1, 2, \dots, n$ . Define  $+$  on  $R[x]$  as follows:

$$\begin{aligned} \alpha + \beta &= (a_1, a_2, a_3, \dots, a_n, 0, \dots) + (b_1, b_2, b_3, \dots, b_n, 0, \dots) \\ &= (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n, 0, \dots). \end{aligned}$$

### Remark:

$(R[x], +)$  is abelian group.

Proof:

1.  $(0, 0, \dots, 0, \dots)$  is the identity.
2.  $\forall \alpha \in R[x], \exists -\alpha \in R[x]$ ,  
where  $-\alpha = (-a_0, -a_1, \dots, -a_n, 0, \dots)$  s.t  $\alpha + (-\alpha) = 0$ .
3. Associative: let  $\alpha, \beta, \gamma \in R[x]$ ,  $\alpha = (a_0, a_1, \dots, a_n, 0, \dots)$ ,  $\beta = (b_0, b_1, \dots, b_n, 0, \dots)$ ,  $\gamma = (c_0, c_1, \dots, c_n, 0, \dots)$ ,  $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$ .
4. Let  $\alpha, \beta \in R[x]$ , then  $\alpha + \beta = (a_0, a_1, \dots, a_n, 0, \dots) + (b_0, b_1, \dots, b_n, 0, \dots) = (a_0 + b_0, a_1 + b_1, \dots, a_n + b_n, 0, \dots) = (b_0 + a_0, b_1 + a_1, \dots, b_n + a_n, 0, \dots)$ . (since  $a_i, b_i \in R$  and  $R$  is commutative), then  $\alpha + \beta = \beta + \alpha$ .

Remark:

$(R[x], +, \cdot)$  is a ring.

Proof:(H.W)

Define  $(\cdot)$  on  $R[x]$  by: If  $\alpha, \beta \in R[x]$ , where  
,  $\alpha = (a_0, a_1, \dots, a_n, 0, \dots)$ ,  $\beta = (b_0, b_1, \dots, b_n, 0, \dots)$ . Then

$\alpha \cdot \beta = (a_0, a_1, \dots, a_n, 0, \dots) \cdot (b_0, b_1, \dots, b_n, 0, \dots) = (c_0, c_1, \dots, c_n, 0, \dots) \in R[x]$ , where  $c_n = \sum_{i+j=n} a_i \cdot b_j$ .

$c_1 = a_0 b_1 + b_0 a_1 \quad \dots \quad c_n = a_0 \cdot b_n + a_1 \cdot b_{n-1} + a_2 \cdot b_{n-2} + \dots + a_n \cdot b_0$

Theorem:

$R$  can be imbedded in  $R[x]$ .

Proof:

If  $S = \{(r, 0, 0, \dots) : r \in R\}$  subset of  $R[x]$

Define  $\phi: R \rightarrow R[x]$  by  $\phi(r) = (r, 0, 0, \dots) \quad \forall r \in R$ .

1.  $\phi$  is homomorphism:

$$\begin{aligned}\phi(r_1 + r_2) &= (r_1 + r_2, 0, 0, \dots) = (r_1, 0, 0, \dots) + (r_2, 0, 0, \dots) \\ &= \phi(r_1) + \phi(r_2)\end{aligned}$$

$$\phi(r_1 \cdot r_2) = (r_1 \cdot r_2, 0, 0, \dots) = (r_1, 0, 0, \dots) \cdot (r_2, 0, 0, \dots) = \phi(r_1) \cdot \phi(r_2)$$

2.  $\phi$  is  $(1 - 1)$ :

If  $\phi(r_1) = \phi(r_2) \Rightarrow (r_1, 0, 0, \dots) = (r_2, 0, 0, \dots)$  iff  $r_1 = r_2$ .

3.  $\phi$  is onto:

Let  $\alpha = (a_0, a_1, \dots, a_n, 0, \dots) \in R[x]$

$$a_0 \in R \Rightarrow \phi(a_0) = (a_0, 0, 0, \dots)$$

$$a_1 \in R \Rightarrow \phi(a_1) = (a_1, 0, 0, \dots)$$

$\vdots$

$$a_n \in R \Rightarrow \phi(a_n) = (a_n, 0, 0, \dots)$$

$$\therefore a_i \in R \Rightarrow \phi(a_i) = (a_i, 0, 0, \dots)$$

### Remark:

Let  $R$  be a ring put  $x = (0, 1, 0, \dots)$ ,  $x^2 = (0, 0, 1, 0, \dots)$ ,  $x^3 = (0, 0, 0, 1, 0, \dots)$ , ...,  $x^n = (0, 0, \dots, 1, 0, \dots)$ .

Let  $(a_0, a_1, \dots, a_n, 0, \dots) \in R[x]$ .

$$\begin{aligned}(a_0, a_1, \dots, a_n, 0, \dots) &= (a_0, 0, \dots) + (0, a_1, 0, \dots) + (0, 0, \dots, a_n, 0, \dots) \\ &= (a_0, 0, \dots) + (0, a_1, 0, \dots) \cdot (0, 1, 0, \dots)x + (0, 0, a_2, 0, \dots) \\ &\quad \cdot (0, 0, 1, 0, \dots)x^2 + \dots + (0, 0, \dots, a_n, 0, \dots)(0, 0, \dots, 1, 0, \dots)x^n \\ &= a_0 + a_1x + a_2x^2 + \dots + a_nx^n\end{aligned}$$

### Definition:

Let  $R$  be a ring and let  $\alpha \in R[x]$  be a nonzero polynomial ring we say that the degree of  $\alpha = n$  [denoted by  $\deg(\alpha) = n$ ] if  $a_n \neq 0$  and  $a_k = 0 \quad \forall k > n$ .

### Examples:

$$\begin{aligned}\alpha(x) &= 5 - x + x^3 - x^5 \in R[x] \\ &= (5, -1, 0, 1, 0, -1, 0, 0, \dots)\end{aligned}$$

$\deg(\alpha) = 5$ ,  $a_5 = -1 \neq 0$  and  $a_k = 0 \quad \forall k < 5$ .

Remark:

If  $\alpha(x) = 0 \in Z[x]$ ,  $\deg(\alpha) = 0$ , then  $\alpha$  is called constant polynomial.

Remark:

If  $R$  is I.D and  $\alpha, \beta \in R[x]$  s.t  $\deg(\alpha(x)) = n$ ,  $\deg(\beta(x)) = m$ . Then  $\deg(\alpha(x) \cdot \beta(x)) = n + m = \deg(\alpha(x)) + \deg(\beta(x))$ .

Definition:

Let  $R$  be a ring and  $R[x]$  be a polynomial ring on  $R$ . Let  $\alpha(x) \in R[x]$  s.t  $\alpha(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ ,  $a_n \neq 0$  we call that  $a_n$  is a leading coefficient of  $\alpha(x)$ , and the integer  $n$  is the degree of  $\alpha$ . If  $a_n = 1$ , then  $\alpha(x)$  is called monic polynomial

Remark:(1)

If  $R$  is a commutative ring, then  $R[x]$  is commutative.

Proof:

Let  $f, g \in R[x]$  s.t

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n, \quad a_n \neq 0$$

$$g(x) = b_0 + b_1x + b_2x^2 + \dots + b_mx^m, \quad b_m \neq 0$$

$$\begin{aligned}f(x) \cdot g(x) &= a_0b_0 + (a_0b_1 + b_0a_1)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \dots \\ &\quad + a_nb_mx^{n+m}\end{aligned}$$

Since  $R$  is a commutative ring, then  $a_ib_j = b_ja_i \quad \forall i, j$ .

$$= b_0 a_0 + \cdots + b_m a_n x^{n+m} = g(x) \cdot f(x)$$

Q:

Is the converse true?

Sol

Yes, since if  $a, b \in R \Rightarrow a, b \in R[x]$ . Put  $f(x) = a$ ,  $g(x) = b$ .

$$\Rightarrow f(x) \cdot g(x) = a \cdot b$$

Since  $R[x]$  is a commutative ring, then  $f \cdot g = g \cdot f \Rightarrow a \cdot b = b \cdot a$ .

$\therefore R$  is a commutative ring.

Remark:(2)

If  $R$  has an identity, then  $R[x]$  has an identity.

Proof:

Since  $R$  has an identity 1, then Put  $f(x) = 1$

$$\therefore \forall g(x) \in R[x] : f(x) \cdot g(x) = g(x) \Rightarrow 1 \cdot g(x) = g(x)$$

Q:

Is the converse true?

Sol

Suppose that  $R[x]$  has an identity say  $f(x)$ .

Now, let  $a \in R$ .

Since  $f(x)$  is the identity of  $R[x]$ .

$$\Rightarrow f(x) \cdot g(x) = g(x) \forall g(x) \in R[x]$$

In special case put  $g(x) = a$ .

$$\Rightarrow f(x) \cdot a = a \Rightarrow f(x) = (1, 0, 0, \dots) = 1.$$

Lemma:

If  $R$  is I.D, then  $R[x]$  is I.D.

Proof:

From the last two remarks. If  $R$  is a commutative ring with 1, then  $R[x]$  is commutative with 1.

Let  $f(x), g(x) \in R[x]$ . s.t

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n, \quad a_n \neq 0$$

$$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m, \quad b_m \neq 0$$

Since  $a_n \neq 0$ ,  $b_m \neq 0$  and  $R$  is I.D, then  $a_n \cdot b_m \neq 0$

$$\Rightarrow f(x) \cdot g(x) \neq 0 \text{ (Since } a_n \cdot b_m \neq 0 \text{)}$$

$\Rightarrow R[x]$  is I. D.

Remark:(3)

Let  $R$  be a commutative ring with one and let  $\alpha, \beta$  be a non zero polynomial in  $R[x]$ , then

$$\deg(\alpha(x) + \beta(x)) \leq \max(\deg \alpha(x), \deg \beta(x)) \text{ or } \alpha(x) + \beta(x) = 0.$$

Example:

$$\alpha(x) = 2 + 3x, \quad \beta(x) = 4 + 3x \quad \text{in } Z_6[x]$$

$$\alpha(x) + \beta(x) = 6 + 6x = 0$$

$$\alpha(x) = 1 + 2x^2, \quad \beta(x) = x \quad \text{in } Z_6[x]$$

$$\alpha(x) + \beta(x) = 1 + x + 2x^2$$

$$\deg(\alpha(x) + \beta(x)) = 2 = \deg \alpha(x)$$

Remark:(4)

$$\deg(\alpha(x) \cdot \beta(x)) \leq (\deg \alpha(x) + \deg \beta(x)) \text{ or } \alpha(x) \cdot \beta(x) = 0.$$

Example:

$$\alpha(x) = 2x, \quad \beta(x) = 3x \quad \text{in } Z_6[x]$$

$$\alpha(x) \cdot \beta(x) = 6x^2 = 0$$

$$\alpha(x) = x, \quad \beta(x) = 1 + x^2 \quad \text{in } Z_6[x]$$

$$\alpha(x) \cdot \beta(x) = x + x^3$$

$$\deg(\alpha(x)) + \deg(\beta(x)) = 1 + 2 =$$

Remark:(5)

If  $R$  is I.D and  $\alpha, \beta \in R[x]$  s.t  $\deg(\alpha(x)) = n$ ,  $\deg(\beta(x)) = m$ , then  
 $\deg(\alpha(x) \cdot \beta(x)) = n + m = \deg(\alpha(x)) + \deg(\beta(x))$ .

Q:

If  $R$  is a field is  $R[x]$  a field?

Sol

(H.W).



**Definition:**

Let  $R$  be a ring, then the function  $f: Z^+ \cup \{0\} \rightarrow R$  is called infinite sequence in  $R$  and we shall denoted to  $f(n)$  by  $r_n$ ,  $\forall n \in Z^+ \cup \{0\}$ .

$r_n$  is called the  $n$ th term (or general term) for thesequence  $\langle r_n \rangle$ .

$$f(n) = (r_0, r_1, \dots, r_n, \dots)$$

**Definition:**

Let  $R$  be a ring, every infinite sequence in  $R$  (all term equal zero except a finite of terms) is called a polynomial ring in  $R$  i. e)  $\exists$  a positive integer  $n$  such that  $r_m = 0 \forall m \geq n$ .

**Examples:**

- (1)  $(0, 0, \dots, 0, \dots)$
- (2)  $(5, 4, -1, 0, 3, 0, 0, \dots)$
- (3)  $(0, 0, 0, -1, 2, 4, 0, 0, \dots)$

Are polynomial rings in  $R$ .

**Remark:**

We will denoted to all polynomial rings in  $R$  by  $R[x]$

$$R[x] = \{(a_1, a_2, a_3, \dots, a_n, 0, 0, \dots) : a_i \in R\}$$

**Remark:**

Let  $\alpha = (a_1, a_2, a_3, \dots, a_n, 0, \dots)$  and  $\beta = (b_1, b_2, b_3, \dots, b_n, 0, \dots)$   $\alpha, \beta \in R[x]$ , then  $\alpha = \beta$  iff  $a_i = b_i \forall i = 1, 2, \dots, n$ . Define  $+$  on  $R[x]$  as follows:

$$\begin{aligned} \alpha + \beta &= (a_1, a_2, a_3, \dots, a_n, 0, \dots) + (b_1, b_2, b_3, \dots, b_n, 0, \dots). \\ &= (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n, 0, \dots). \end{aligned}$$

**Remark:**

$(R[x], +)$  is abelian group.

Proof:

1.  $(0, 0, \dots, 0, \dots)$  is the identity.
2.  $\forall \alpha \in R[x], \exists -\alpha \in R[x]$ ,  
where  $-\alpha = (-a_0, -a_1, \dots, -a_n, 0, \dots)$  s.t  $\alpha + (-\alpha) = 0$ .
3. Associative: let  $\alpha, \beta, \gamma \in R[x]$ ,  $\alpha = (a_0, a_1, \dots, a_n, 0, \dots)$ ,  $\beta = (b_0, b_1, \dots, b_n, 0, \dots)$ ,  $\gamma = (c_0, c_1, \dots, c_n, 0, \dots)$ ,  $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$ .
4. Let  $\alpha, \beta \in R[x]$ , then  $\alpha + \beta = (a_0, a_1, \dots, a_n, 0, \dots) + (b_0, b_1, \dots, b_n, 0, \dots) = (a_0 + b_0, a_1 + b_1, \dots, a_n + b_n, 0, \dots) = (b_0 + a_0, b_1 + a_1, \dots, b_n + a_n, 0, \dots)$ . (since  $a_i, b_i \in R$  and  $R$  is commutative), then  $\alpha + \beta = \beta + \alpha$ .

Remark:

$(R[x], +, \cdot)$  is a ring.

Proof:(H.W)

Define  $(\cdot)$  on  $R[x]$  by: If  $\alpha, \beta \in R[x]$ , where  
 $\alpha = (a_0, a_1, \dots, a_n, 0, \dots)$ ,  $\beta = (b_0, b_1, \dots, b_n, 0, \dots)$ . Then

$\alpha \cdot \beta = (a_0, a_1, \dots, a_n, 0, \dots) \cdot (b_0, b_1, \dots, b_n, 0, \dots) = (c_0, c_1, \dots, c_n, 0, \dots) \in R[x]$ , where  $c_n = \sum_{i+j=n} a_i \cdot b_j$ .

$c_1 = a_0 b_1 + b_0 a_1 \quad \dots \quad c_n = a_0 \cdot b_n + a_1 \cdot b_{n-1} + a_2 \cdot b_{n-2} + \dots + a_n \cdot b_0$

Theorem:

$R$  can be imbedded in  $R[x]$ .

Proof:

If  $S = \{(r, 0, 0, \dots) : r \in R\}$  subset of  $R[x]$

Define  $\phi: R \rightarrow R[x]$  by  $\phi(r) = (r, 0, 0, \dots) \quad \forall r \in R$ .

1.  $\phi$  is homomorphism:

$$\begin{aligned}\phi(r_1 + r_2) &= (r_1 + r_2, 0, 0, \dots) = (r_1, 0, 0, \dots) + (r_2, 0, 0, \dots) \\ &= \phi(r_1) + \phi(r_2)\end{aligned}$$

$$\phi(r_1 \cdot r_2) = (r_1 \cdot r_2, 0, 0, \dots) = (r_1, 0, 0, \dots) \cdot (r_2, 0, 0, \dots) = \phi(r_1) \cdot \phi(r_2)$$

2.  $\phi$  is  $(1 - 1)$ :

If  $\phi(r_1) = \phi(r_2) \Rightarrow (r_1, 0, 0, \dots) = (r_2, 0, 0, \dots)$  iff  $r_1 = r_2$ .

3.  $\phi$  is onto:

Let  $\alpha = (a_0, a_1, \dots, a_n, 0, \dots) \in R[x]$

$$a_0 \in R \Rightarrow \phi(a_0) = (a_0, 0, 0, \dots)$$

$$a_1 \in R \Rightarrow \phi(a_1) = (a_1, 0, 0, \dots)$$

$$\vdots$$

$$a_n \in R \Rightarrow \phi(a_n) = (a_n, 0, 0, \dots)$$

$$\therefore a_i \in R \Rightarrow \phi(a_i) = (a_i, 0, 0, \dots)$$

### Remark:

Let  $R$  be a ring put  $x = (0, 1, 0, \dots)$ ,  $x^2 = (0, 0, 1, 0, \dots)$ ,  $x^3 = (0, 0, 0, 1, 0, \dots)$ , ...,  $x^n = (0, 0, \dots, 1, 0, \dots)$ .

Let  $(a_0, a_1, \dots, a_n, 0, \dots) \in R[x]$ .

$$\begin{aligned}(a_0, a_1, \dots, a_n, 0, \dots) &= (a_0, 0, \dots) + (0, a_1, 0, \dots) + (0, 0, \dots, a_n, 0, \dots) \\ &= (a_0, 0, \dots) + (0, a_1, 0, \dots) \cdot (0, 1, 0, \dots)x + (0, 0, a_2, 0, \dots) \\ &\quad \cdot (0, 0, 1, 0, \dots)x^2 + \dots + (0, 0, \dots, a_n, 0, \dots)(0, 0, \dots, 1, 0, \dots)x^n \\ &= a_0 + a_1x + a_2x^2 + \dots + a_nx^n\end{aligned}$$

### Definition:

Let  $R$  be a ring and let  $\alpha \in R[x]$  be a nonzero polynomial ring we say that the degree of  $\alpha = n$  [denoted by  $\deg(\alpha) = n$ ] if  $a_n \neq 0$  and  $a_k = 0 \quad \forall k > n$ .

### Examples:

$$\begin{aligned}\alpha(x) &= 5 - x + x^3 - x^5 \in R[x] \\ &= (5, -1, 0, 1, 0, -1, 0, 0, \dots)\end{aligned}$$

$$\deg(\alpha) = 5, a_5 = -1 \neq 0 \text{ and } a_k = 0 \quad \forall k < 5.$$

Remark:

If  $\alpha(x) = 0 \in Z[x]$ ,  $\deg(\alpha) = 0$ , then  $\alpha$  is called constant polynomial.

Remark:

If  $R$  is I.D and  $\alpha, \beta \in R[x]$  s.t  $\deg(\alpha(x)) = n$ ,  $\deg(\beta(x)) = m$ . Then  $\deg(\alpha(x) \cdot \beta(x)) = n + m = \deg(\alpha(x)) + \deg(\beta(x))$ .

Definition:

Let  $R$  be a ring and  $R[x]$  be a polynomial ring on  $R$ . Let  $\alpha(x) \in R[x]$  s.t  $\alpha(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ ,  $a_n \neq 0$  we call that  $a_n$  is a leading coefficient of  $\alpha(x)$ , and the integer  $n$  is the degree of  $\alpha$ . If  $a_n = 1$ , then  $\alpha(x)$  is called monic polynomial

Remark:(1)

If  $R$  is a commutative ring, then  $R[x]$  is commutative.

Proof:

Let  $f, g \in R[x]$  s.t

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n, \quad a_n \neq 0$$

$$g(x) = b_0 + b_1x + b_2x^2 + \dots + b_mx^m, \quad b_m \neq 0$$

$$\begin{aligned}f(x) \cdot g(x) &= a_0b_0 + (a_0b_1 + b_0a_1)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \dots \\ &\quad + a_nb_mx^{n+m}\end{aligned}$$

Since  $R$  is a commutative ring, then  $a_ib_j = b_ia_i \quad \forall i, j$ .

$$= b_0 a_0 + \cdots + b_m a_n x^{n+m} = g(x) \cdot f(x)$$

Q:

Is the converse true?

Sol

Yes, since if  $a, b \in R \Rightarrow a, b \in R[x]$ . Put  $f(x) = a$  ,  $g(x) = b$  .

$$\Rightarrow f(x) \cdot g(x) = a \cdot b$$

Since  $R[x]$  is a commutative ring, then  $f \cdot g = g \cdot f \Rightarrow a \cdot b = b \cdot a$  .

$\therefore R$  is a commutative ring.

Remark:(2)

If  $R$  has an identity, then  $R[x]$  has an identity.

Proof:

Since  $R$  has an identity 1, then Put  $f(x) = 1$

$$\therefore \forall g(x) \in R[x] : f(x) \cdot g(x) = g(x) \Rightarrow 1 \cdot g(x) = g(x)$$

Q:

Is the converse true?

Sol

Suppose that  $R[x]$  has an identity say  $f(x)$ .

Now, let  $a \in R$ .

Since  $f(x)$  is the identity of  $R[x]$ .

$$\Rightarrow f(x) \cdot g(x) = g(x) \forall g(x) \in R[x]$$

In special case put  $g(x) = a$  .

$$\Rightarrow f(x) \cdot a = a \Rightarrow f(x) = (1, 0, 0, \dots) = 1 .$$

Lemma:

If  $R$  is I.D, then  $R[x]$  is I.D.

Proof:

From the last two remarks. If  $R$  is a commutative ring with 1, then  $R[x]$  is commutative with 1.

Let  $f(x), g(x) \in R[x]$ . s.t

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n, \quad a_n \neq 0$$

$$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m, \quad b_m \neq 0$$

Since  $a_n \neq 0$ ,  $b_m \neq 0$  and  $R$  is I.D, then  $a_n \cdot b_m \neq 0$

$$\Rightarrow f(x) \cdot g(x) \neq 0 \text{ (Since } a_n \cdot b_m \neq 0 \text{)}$$

$\Rightarrow R[x]$  is I. D.

Remark:(3)

Let  $R$  be a commutative ring with one and let  $\alpha, \beta$  be a non zero polynomial in  $R[x]$ , then

$$\deg(\alpha(x) + \beta(x)) \leq \max(\deg \alpha(x), \deg \beta(x)) \text{ or } \alpha(x) + \beta(x) = 0.$$

Example:

$$\alpha(x) = 2 + 3x, \quad \beta(x) = 4 + 3x \quad \text{in } Z_6[x]$$

$$\alpha(x) + \beta(x) = 6 + 6x = 0$$

$$\alpha(x) = 1 + 2x^2, \quad \beta(x) = x \quad \text{in } Z_6[x]$$

$$\alpha(x) + \beta(x) = 1 + x + 2x^2$$

$$\deg(\alpha(x) + \beta(x)) = 2 = \deg \alpha(x)$$

Remark:(4)

$$\deg(\alpha(x) \cdot \beta(x)) \leq (\deg \alpha(x) + \deg \beta(x)) \text{ or } \alpha(x) \cdot \beta(x) = 0.$$

Example:

$$\alpha(x) = 2x, \quad \beta(x) = 3x \quad \text{in } Z_6[x]$$

$$\alpha(x) \cdot \beta(x) = 6x^2 = 0$$

$$\alpha(x) = x, \quad \beta(x) = 1 + x^2 \quad \text{in } Z_6[x]$$

$$\alpha(x) \cdot \beta(x) = x + x^3$$

$$\deg(\alpha(x)) + \deg(\beta(x)) = 1 + 2 =$$

Remark:(5)

If  $R$  is I.D and  $\alpha, \beta \in R[x]$  s.t  $\deg(\alpha(x)) = n$ ,  $\deg(\beta(x)) = m$ , then  
 $\deg(\alpha(x) \cdot \beta(x)) = n + m = \deg(\alpha(x)) + \deg(\beta(x))$ .

Q:

If  $R$  is a field is  $R[x]$  a field?

Sol

(H.W).

Theorem:(Division Algorithm)

Let  $R$  be a commutative ring with 1 and  $f(x), g(x) \neq 0$  be two polynomials in  $R[x]$  with leading coefficient of  $g(x)$  an invertible element. Then there exist unique polynomial  $q(x), r(x) \in R[x]$  s.t

$$f(x) = q(x) \cdot g(x) + r(x)$$

Where either  $r(x) = 0$  or  $\deg(r(x)) < \deg(g(x))$ .

Proof:

If  $f(x) = 0$  we will take  $q(x) = r(x) = 0$

$$r(x) = f(x) = 0 \cdot g(x) \neq 0$$

If  $\deg(f(x)) < \deg(g(x))$  we will take  $q(X) = 0$  and  $r(X) = f(x)$ .

$$f(x) = g(x).0 + f(x) ; f(x) = r(x)$$

Notice that  $\deg(r(x)) = \deg(f(x)) < \deg(g(x))$

Now suppose that  $f(x) \neq 0$  and  $\deg(f(x)) \leq \deg(g(x))$ .

By induction on  $\deg(f(X))$ .

1) Suppose that  $\deg(f(x)) = 0$

$$i.e) f(x) = c , c \neq 0 \in R$$

$$\therefore \deg(f(x)) \geq \deg(g(x)) \rightarrow \deg(g(x)) = 0$$

$$i.e) g(x) = k , R \ni k \neq 0$$

$$c = c \cdot k^{-1} \cdot k + 0 \text{ [since the coefficient of } g \text{ is invertible].}$$

Suppose that the theorem is true for all polynomial.

Which its degree less than degree  $f(x)$

$$f(x) = a_0 + a_1x + \cdots a_nx^n , a_n \neq 0$$

$$g(x) = b_0 + b_1x + \cdots b_mx^m , b_m \neq 0 .$$

$$\text{Put } f_1(x) = f(x) - (a_nb_m^{-1})x^{n-m} \cdot g(x) \quad \dots (1)$$

$$\deg(f(x)) \geq \deg f_1(x)$$

$\therefore$  by induction  $\exists q_1(x), r(x)$  satisfy

$$f_1(x) = g(x).q_1(x) + r(x) \quad \dots (2)$$

And either  $r(x) = 0$  or  $\deg(r(x)) < \deg g(x)$ .

Sub.(2) in (1) we get :-

$$g(x).q_1(x) + r(x) = f(x) - (a_nb_m^{-1}) \cdot x^{n-m} \cdot g(x)$$

$$f(x) = (q_1(x) + a_nb_m^{-1} \cdot x^{n-m}).g(x) + r(x)$$



By (2)  $r(x) = 0$  or  $\deg(r(x)) < \deg(g(x))$ .

Uniqueness:- Suppose that there exist  $q_1(x), r_1(x) \in R[x]$  s.t

$$f(x) = q_1(x).g(x) + r_1(x), \\ \deg r_1(x) = 0 \text{ or } \deg r_1(x) < \deg g(x)$$

Put  $f(x) = q(x).g(x) + r(x)$  and  $r(x) = 0$  or  $\deg r(x) < \deg g(x)$ .

$$q(x).g(x) + r(x) = q_1(x).g(x) + r_1(x)$$

$$(q(x) - q_1(x)).g(x) = r_1(x) - r(x) \quad \dots (*)$$

If  $q \neq q_1 \rightarrow q(x) \neq q_1(x) \quad \forall x \in R \rightarrow q(x) - q_1(x) \neq 0 \quad \forall x \in R$

$$\rightarrow \deg(q(x) - q_1(x)).g(x) = \deg(q(x) - q_1(x)) + \deg(g(x)) \\ = \deg(r(x) - r_1(x)) \text{ by } (*)$$

Put  $\deg(r(x) - r_1(x)) \leq \max\{\deg(r(x)), \deg(r_1(x))\}$ .

$$\max\{\deg(r(x)), \deg(r_1(x))\} \geq \deg(g(x)) + \deg(q(x) - q_1(x)) \quad C!$$

With  $\deg(r(x)) < \deg(g(x))$  and  $\deg(r_1(x)) < \deg(g(x))$ .

$$\therefore q \neq q_1 \rightarrow q(x) \neq q_1(x) \quad \forall x \rightarrow q(x) - q_1(x) \neq 0 \quad \forall x \in R$$

$$\therefore r(x) - r_1(x) = 0 \quad \forall x \rightarrow r(x) = r_1(x) \quad \forall x \in R \quad \therefore r = r_1.$$

$\therefore q$  and  $r$  are unique.

### Example:

Let  $f(x) = 3x^3 + 2x^2 + 1$ ,  $g(x) = x^2 - 1$  find  $q, r$ .

**Sol:**  $q(x) = 3x + 2$ ,  $r(x) = 3x + 3$

$$f(x) = q(x).g(x) + r(x)$$

### Definition:

Let  $R$  be a ring with  $1$ , then a ring  $R'$  is called extension for  $R$  if  $R'$  contain  $R$  as a subring ( $R \subset R'$ )

**Theorem:**

Let  $R$  be a commutative ring with 1 s.t.  $R$  is imbedded in  $\acute{R}$  and let  $f(x) \in R[x]$

$f(x) = a_0 + a_1x + \cdots + a_n x^n$ ,  $a_n \neq 0$  and let  $r \in \text{cent } \acute{R}$ , then  $\exists$  a ring homomorphism.

$\varphi_r: R[x] \rightarrow \acute{R}$  define by  $\varphi_r(f(x)) = f(r)$ .

$$f(r) = a_0 + a_1r + \cdots + a_nr^n \in \acute{R}$$

**Proof:**

$$f(x) = a_0 + a_1x + \cdots + a_n x^n, \quad a_n \neq 0$$

$$g(x) = b_0 + b_1x + \cdots + b_mx^m, \quad b_m \neq 0 \quad n > m$$

$$\varphi_r(f(x) + g(x))$$

$$= \varphi_r[(a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_m + b_m)x^m + \cdots + a_n x^n]$$

$$= a_0 + b_0 + (a_1 + b_1)r + \cdots + (a_m + b_m)r^m + \cdots + a_nr^n$$

$$= f(r) + g(r) = \varphi_r(f(x)) + \varphi_r(g(x))$$

$$\varphi_r(f(x) \cdot g(x)) = \varphi_r[(a_0b_0) + (a_0b_1 + a_1b_0)x + \cdots + a_nb_mx^{n+m}]$$

$$= (a_0b_0) + (a_0b_1 + a_1b_0)r + \cdots + a_nb_mr^{n+m}$$

$$= f(r) \cdot g(r)$$

$\therefore \varphi_r$  is a ring homomorphism.

**Definition:**

Let  $R$  be a commutative ring with 1 and let  $\acute{R}$  be an extension of  $R$  and let  $r \in \text{cent } \acute{R}$ , we denote the set

$$\varphi_r = \varphi_r(R[x]) = \{f(r) : f(x) \in R[x]\}$$

Examp<sub>l</sub>s:

1. In  $(Z, +, \cdot)$ .

$$f(x) = 1 + 2x, \quad g(x) = 2 + 3x + 4x^2$$

$$\deg(f \cdot g) = 2 + 1 = 3 \quad [\text{since } a_n \cdot b_m \neq 0]$$

2. In  $(Z_n, +, \cdot)$ .

$$f(x) = \bar{1} + \bar{3}x + \bar{2}x^2, \quad g(x) = \bar{5} + \bar{6}x + \bar{4}x^2 + \bar{6}x^3$$

$$\deg(f \cdot g) = \bar{5} \text{ false}$$

$$[\text{since } a_n = \bar{2}, b_m = \bar{6}, a_n \cdot b_m = \bar{2} \cdot \bar{6} = 12 = \bar{0}]$$

$$\therefore \deg(f \cdot g) = \bar{4}$$

Lemma:

Let  $R$  be a commutative ring with 1  $f(x) = a_0 + a_1x + \dots + a_nx^n$ ,  
 $g(x) = b_0 + b_1x + \dots + b_mx^m$  s.t  $b_m$  has inverse, then  
 $\deg(f \cdot g) = \deg(f) + \deg(g)$ ,  $a_n \neq 0$ ,  $b_m \neq 0$

Proof:

Suppose that  $[a_n \cdot b_m = 0] \cdot b_m^{-1} \rightarrow a_n = 0$  C!  $\rightarrow a_n \cdot b_m \neq 0$

Examp<sub>l</sub>:

$$f(x) = 6x + 3x^2 + 5x^3 + 6x^6, \quad g(x) = 6 + 5x^2 + 5x^{10} \text{ in } R$$

5 invertible.

**(Division Algorithm)**

1-  $R$  commutative ring with 1 2-  $f, g \neq 0$  3-  $b_m$  invertible in  $R$ . Then  
 $\exists! q, r \in R[x]$  s.t  $f = q \cdot g + r$  and  $r = 0$  or  $\deg(r) < \deg(g)$ .

Examp<sub>l</sub>s:

1.  $R = Z$ , polynomial in  $Z[x]$ .

$$f(x) = x^6 + 3x^5 + 2x^4, \quad g(x) = 6 + 5x + x^2$$

1-  $Z$  commutative ring with 1 2-  $f, g \neq 0$  3-  $b_m = 1$  invertible in  $Z$ .

Then  $\exists! q(x), r(x) \in R[x]$  s.t  $f(x) = q(x).g(x) + r(x)$  and  $r(x) = 0$  or  $\deg(r(x)) < \deg(g(x))$

2  $R = Z$  , polynomial in  $Z[x]$ .

$$f(x) = x^6 + 3x^5 + 4x^3 - 3x + 2, \quad g(x) = x^2 + 3x - 4$$

1-  $Z$  commutative ring with 1 2-  $f, g \neq 0$  3-  $b_m = -4$  invertible in  $Z$ .

Then  $\exists! q(x), r(x) \in R[x]$  s.t  $f(x) = q(x).g(x) + r(x)$  and  $r(x) = 0$  or  $\deg(r(x)) < \deg(g(x))$

### Remark:

If  $f(r) = 0$  , then  $r \in R$  is called a root of  $f(x)$ .

### Theorem: (Remainder theorem)

Let  $R$  be a commutative ring with 1, if  $f(x) \in R[x]$  ,  $a \in R$  then there exist unique polynomial  $q(x) \in R[x]$  s.t

$$f(x) = (x - a)q(x) + f(a).$$

### Proof:

Let  $g(x) = x - a$  , then by division algorithm (for  $f(x)$  and  $x - a$ )  $\exists$  unique  $r(x), q(x) \in R[x]$  s.t  $f(x) = (x - a)q(x) + r(x) \dots (1)$

And either  $r(x) = 0$  or  $\deg(r(x)) < \deg(x - a)$

But  $\deg(x - a) = 1 \rightarrow \deg(r(x)) = 0 \rightarrow r(x) = c$  .

Sub  $r(x)$  in (1) we get  $f(x) = (x - a)q(x) + c$  .

Put  $x = a \rightarrow f(a) = (a - a)q(a) + c \rightarrow f(a) = c$  .

$$\therefore f(x) = (x - a)q(x) + f(a)$$

Example

Let  $f(x) = x^3 + 5x^2 + x + 1$ ,  $g(x) = x - 1$ ?

Corollary:

Let  $R$  be a commutative ring with 1,  $f(x) \in R[x]$ ,  $a \in R$ , then  $(x - a)$  is divisible  $f(x)$  iff  $a$  is a root of  $f(x)$ .

Proof:  $\Rightarrow$ 

$\because (x - a) \mid f(x) \rightarrow f(x) = (x - a)g(x)$  where  $g(x) \in R[x]$ .

$$f(a) = (a - a) \cdot g(a) = 0 \rightarrow a \text{ is a root of } f(x)$$

$\Leftarrow$ ) Let  $f(a) = 0$  by Remainder theorem  $\exists! q(x) \in R[x]$  s.t  $f(x) = (x - a)q(x) + f(a)$ .

$$f(x) = (x - a) \cdot q(x) \text{ [since } f(a) = 0]$$

$$\therefore (x - a) \mid f(x).$$

Theorem:

Let  $R$  be an I.D and  $0 \neq f(x) \in R[x]$  be a polynomial of degree  $n$ , then  $f$  has at most  $n$  distinct roots in  $R$ .

Proof:

By induction on  $\deg(f(x))$  if  $\deg f(x) = 0 \rightarrow f(x) = c$ ,  $0 \neq c \in R$   
 $\rightarrow f$  has no root.

If  $\deg(f(x)) = 1 \rightarrow f(x) = ax + b$  where  $a, b \in R$

If  $a$  is an invertible element in  $R \rightarrow$  the root of  $f(x)$  is  $(-ba^{-1})$

$$, f(-ba^{-1}) = a(-ba^{-1}) + b = 0$$

If  $a$  has no inverse then  $\rightarrow f$  has no root

Now suppose that the theorem is true for every polynomial with degree less than  $n$ .

Let  $\deg(f(x)) = n$ . (if  $f$  has no roots then the theorem is true).

Let  $a \in R$ , if  $a$  is a root of  $f(x)$  then by last corr.  $\rightarrow (x - a)/f(x) \rightarrow f(x) = (x - a)q(x)$ ;  $q(x) \in R[x]$ .

$$\deg(f(x)) = \deg((x - a)q(x))$$

$$= \deg(x - a) + \deg(q(x)) \quad [\text{since } R \text{ is I.D}]$$

$$n = 1 + \deg(q(x)) \rightarrow \deg(q(x)) = n - 1$$

$\therefore$  By induction  $q$  has at most  $(n - 1)$  of roots and since  $(x - a)$  has one root

$\therefore f(x)$  has  $n$  distinct roots.

### Corollary:

let  $R$  be an I.D and let  $f(x), g(x) \in R[x]$  are two polynomial of degree  $n$ , if  $\exists (n + 1)$  roots of distinct elements  $a_k \in R$  s.t

$$f(a_k) = g(a_k) \quad \forall k = 1, 2, \dots, n + 1, \text{ then } f(x) = g(x) \quad \forall x$$

### Proof:

$$\text{Let } h(x) = f(x) - g(x), \quad \deg(h(x)) \leq n$$

$\therefore \exists$  at least  $n + 1$  of element for  $h(x)$  [theorem]

$$\text{s.t } h(a_k) = 0, \quad k = 1, 2, \dots, n + 1.$$

$$0 = h(a_k) = f(a_k) - g(a_k), \quad k = 1, \dots, n + 1.$$

$\therefore h$  has more than  $n$  roots C!  $\rightarrow h(x) = 0 \quad \forall x$ .

$$\therefore f(x) - g(x) = 0 \rightarrow f(x) = g(x).$$

### Corollary:

Let  $R$  be an I.D and  $f(x) \in R[x]$  and let  $S$  be any infinite subset of  $R$ .  
If  $f(a) = 0 \quad \forall a \in S$ , then  $f$  is the zero polynomial.

**Proof:**

Suppose that  $f(x)$  is a polynomial of degree  $n$ , then by last theorem  $f$  has at most  $n$  roots C!

Since  $f(a) = 0 \quad \forall a \in S$  and  $S$  is infinite set  $\rightarrow f(x) = 0 \quad \forall x$ .

**Theorem:**

Let  $F$  be a field, then  $F[x]$  is E.D

**Proof:**

$\because F$  is a field  $\rightarrow F$  is I.D  $\rightarrow F[x]$  is I.D.

Now define  $\delta: F[x] \rightarrow Z^+ \cup \{0\}$

$$\delta(f(X)) = \begin{cases} 0 & \text{if } f(x) = 0 \\ 2^{\deg(f(x))} & \text{if } f(x) \neq 0 \end{cases}$$

$$(1) \quad \delta(f(x)) = 0 \text{ if } f(x) = 0$$

$$(2) \quad \delta(f(x).g(x)) = 2^{\deg(f(x).g(x))}$$

$$= 2^{\deg(f(x)+\deg g(x))} [\text{since } R \text{ is I.D}]$$

$$= 2^{\deg(f(x))} \cdot 2^{\deg(g(x))}.$$

$$= \delta(f(x)) \cdot \delta(g(X)).$$

(3) let  $f(x), g(x) \in F[x]$  by division algorithm,  $\exists$  unique  $r(x), q(x) \in F[x]$  s.t  $f(x) = q(x).g(x) + r(x)$  and either  $r(x) = 0$  or  $\deg(r(x)) < \deg(g(x))$

Case(1) if  $r(x) = 0 \rightarrow \delta(r(x)) = 0 < \delta(g(x)) = 2^{\deg(g(x))}$ .

Case(2)  $r(x) \neq 0 \rightarrow \delta(r(x)) = 2^{\deg(r(x))}$



$$\therefore \deg(r(x)) < \deg(g(x)).$$

$$2^{\deg(r(x))} < 2^{\deg(g(x))}.$$

$$\delta(r(x)) < \delta(g(x)),$$

$$\therefore F[x] \text{ is E.D.}$$

### Corollary:

Let  $F$  be a field, then  $F[x]$  is P.I.D.

### Proof:

$F$  is a field  $\rightarrow F[x]$  is E.D.  $\rightarrow F[x]$  is a P.I.D [ Every E.D. is P.I.D]

### Corollary:

If  $F$  is a field, then  $F[x]$  is U.F.D.

### Proof:

$F$  is a field  $\rightarrow F[x]$  is E.D.  $\rightarrow F[x]$  is P.I.D.  $\rightarrow F[x]$  is U.F.D.

### Theorem:

Let  $R$  be I.D and let  $g(x)$  be a polynomial which is not constant in  $R[x]$ , we say that  $g(x)$  is irreducible if we cannot find two polynomials  $h(x), k(x) \in R[x]$  s.t  $g(x) = h(x).k(x)$  and satisfies that  $h(x), k(x)$  with positive degree not equal zero.

Otherwise we say that  $g(x)$  is reducible polynomial.

### Example:

$f(x) = 2x^2 - 4$  in  $Z[x]$   $\rightarrow f(x) = 2(x^2 - 2) = 2(x - \sqrt{2})(x + \sqrt{2})$   
and  $x - \sqrt{2} \notin Z[x]$   $\rightarrow f(x)$  is irreducible.

### Remark(1):

- (1) The reducible polynomial must be of degree greater or equal two.
- (2) All polynomial of first degree is irreducible.
- (3) The constant polynomial cannot be considered reducible or irreducible by definition.

Q/ prove that  $\langle x \rangle$  in  $Z[x]$  is prime not maximal ideal.

**Proof:**

$$\langle x \rangle = \{xf(x) : f(x) \in Z[x]\}, \quad x \in Z$$

$$\langle x \rangle \neq Z[x]?$$

$$\because ax + b \in Z[x], \quad b \neq 0$$

$$\text{but } ax + b \notin \langle x \rangle$$

$$\therefore \langle x \rangle \neq Z[x].$$

(2) Define  $\varphi : Z[x] \rightarrow Z$  by:  $\varphi(f(x)) = f(0)$

$\varphi$  is onto and homomorphism?

$$\therefore \text{By F.I.T } \frac{Z[x]}{\ker \varphi} \cong Z$$

$$\ker \varphi = \{f(x) \in Z[x] : \varphi(f(x)) = 0\}$$

$$= \{f(x) \in Z[x] : f(0) = 0\} = \langle x \rangle$$

$$\therefore \frac{Z[x]}{\langle x \rangle} \cong Z \quad \text{but } Z \text{ is I.D then by [theorem]}$$

$$\therefore \frac{Z[x]}{\langle x \rangle} \text{ is I.D thus } \langle x \rangle \text{ is prime by } [I \text{ is prime iff } \frac{R}{I} \text{ is I.D.}]..$$

Now if we suppose that  $\langle x \rangle$  is maximal ideal then by theorem

$$[I \text{ is maximal ideal iff } \frac{R}{I} \text{ is a field}]$$

$\rightarrow \therefore \frac{Z[x]}{\langle x \rangle}$  is a field  $\rightarrow Z$  is a field C! since  $Z$  is not a field.

Q: Is  $Z[x]$  P.I.D?

Sol/No, since if  $Z[x]$  is P.I.D and  $Z$  is I.D  $\rightarrow$  by the last theorem  $Z$  is a field C!

Corollary(2):

If  $f(x) \in R[x]$  with positive degree, then  $f(x)$  can be written as a product of linear factors and others with constant degree.

proof::

Let  $f(x) \in R[x]$  by last corollary

$$f(x) = (x - c_1)(x - c_2) \dots (x - c_n)$$

, if  $c_i \in R \rightarrow x - c_i \in R[x] \rightarrow$  the proof is finish

Now, if

$c_j \in C \rightarrow c_j = a_j + ib_j$  ,  $a_j, b_j \in R$  , if  $c_j$  is a root, then  $\bar{c}_j$  is a root

$$\bar{c}_j = a_j - ib_j .$$

$$\text{Now, } (x - c_j)(x - \bar{c}_j) = [x - (a_j + ib_j)][x - (a_j - ib_j)]$$

$$= x^2 - 2a_jx + (a_j^2 + b_j^2) \in R[x] \quad C!$$

Example:

$$f(x) = x^4 + x^2 + 1 \in R[x] , \text{ has no root in } R$$

Lemma:

Let  $F$  be a field, then the following are equivalent:

- (1)  $f(x)$  is an irreducible polynomial in  $F[x]$ .
- (2) The principle ideal  $\langle f(x) \rangle$  is a maximal or prime ideal in  $F[x]$ .
- (3) The quotient ring  $\frac{F[x]}{\langle f(x) \rangle}$  is a field

Proof:(H.W)Example:

Let  $f(x) = x^2 + 1$  is  $f(x)$  irreducible in  $R[x]$  ? i. e). Is  $\langle x^2 + 1 \rangle$  maximal ideal?

If it's maximal  $\rightarrow f(x)$  is irreducible in  $R[x]$

$$\frac{R[x]}{\langle x^2 + 1 \rangle} \cong C \quad ?$$

$\therefore C$  field  $\rightarrow \frac{R[x]}{\langle x^2 + 1 \rangle}$  is field iff  $\langle x^2 + 1 \rangle$  is maximal ideal.

$\therefore f(x) = x^2 + 1$  is irreducible. [by last Lemma]

### Theorem:

If  $R$  is U.F.D, then  $R[x]$  is U.F.D

**Proof:**(H.W)

### Definition:

Let  $R$  be U.F.D "the content" of non constant polynomial

$f(x) = a_0 + a_1x + \dots + a_nx^n \in R[x]$ . denoted by symbol  $\text{cont } f(x)$ , is defined to be a greatest common divisor of its coefficient.

(i. e)  $\text{cont } f(x) = \text{g.c.d.}(a_0, \dots, a_n)$ .

(\*) If  $\text{cont } f(x) = 1$ , then we called  $f(x)$  primitive polynomial.

### Example:

$$4x^3 - 32x^2 - 16, \quad \text{cont } f(x) = \text{g.c.d.}(4, -32, -16) = 4$$

### Example:

$$f(x) = 3x^5 - 5x^2 + 7x + 1, \quad \text{cont } f(x) = 1.$$

$\therefore f(x)$  is primitive.

### Remarks:

- (1)  $f(x) \in Z[x]$  is primitive iff there is no prime number  $p$  divided all coefficient  $a_i$  of  $f(x)$ .
- (2) Let  $f(x)$  be a polynomial not primitive, then there exists a primitive polynomial  $f_1(x) \in Z[x]$  s.t  $f(x) = \text{cont } f(x) \cdot f_1(x)$ .
- (3) If  $f(x) \in Z[x]$  with positive degree, then  $f(x) = \text{cont } (f(x)) \cdot f_1(x)$  where  $f_1(x)$  is primitive.

### Gaus Theorem:

If  $f(x), g(x)$  are primitive polynomials in  $Z[x]$ , then  $f(x) \cdot g(x)$  is also primitive polynomial in  $Z[x]$ .

### Proof:

Let  $f(x) = a_0 + a_1x + \dots + a_nx^n \in R[x]$  ,  $a_n \neq 0$  and

$g(x) = b_0 + b_1x + \dots + b_mx^m \in R[x]$  ,  $b_m \neq 0$  . Let

$$h(x) = f(x) \cdot g(x)$$

Suppose that  $h(x)$  is not primitive.

$\therefore \exists p$  a prime number s.t  $p$  divide all the coefficient of  $h(x)$  ... (1)  
and  $p$  not divide all  $a_i$  (since  $f$  is primitive).

Suppose  $k$  is the smallest positive integer s.t  $p \nmid a_k$ , and  $p$  not divide all  $b_j$  [since  $g$  is primitive], let  $l$  be the smallest positive integer s.t  $p \nmid b_l$  ... (2).

Now, let  $h(x) = c_0 + c_1x + \dots + a_{k+1}x^{k+1} + \dots + a_{n+m}x^{n+m}$

$$p \nmid c_i \quad \forall i \rightarrow p \nmid c_{k+l}$$

$$\begin{aligned}
c_{k+l} &= \sum_{i+j} a_i b_j \\
&= a_0 b_{k+l} + a_1 b_{k+l-1} + \cdots + a_{k-1} b_{l+1} + a_k b_l + a_{k+1} b_{l-1} + \cdots \\
&\quad + a_{k+l} b_0
\end{aligned}$$

For choice of  $k$  and  $l$   $p \nmid a_{k+1} b_{l-1} + \cdots + a_{k+1} b_0$  and  $p \nmid c_{k+l} \rightarrow p \nmid a_k b_l$  but  $p$  is prime number  $\therefore p \nmid a_k$  or  $p \nmid b_l$   $C!$  with (1) and (2)  $\therefore h(x)$  is primitive polynomial.

### Corollary:

If each  $f(x)$  and  $g(x) \in Z[x]$  are polynomial with positive degree. Then  $\text{cont}(f(x).g(x)) = \text{cont } f(x). \text{cont } g(x)$

### Proof:

In case  $f$  and  $g$  are both primitive polynomial.

$$\therefore \text{cont.}(f(x).g(x)) = 1, \therefore \text{cont.}(f(x)) = 1 \text{ and } \text{cont.}(g(x)) = 1$$

$$\therefore \text{cont.}(f(x).g(x)) = 1 = 1.1 = \text{cont}(f(x)).\text{cont}(g(x)).$$

Now suppose that  $f$  and  $g$  are not primitive.

Let  $\text{cont}(f(x)) = a$  and  $\text{cont } g(x) = b$ ,  $0 \neq a, b \in Z$ .

By remark (2)  $\exists f_1(x), g_1(x)$  primitive polynomial s.t  $f(x) = \text{cont. } f(x) f_1(x)$  and  $g(x) = \text{cont } g(x) g_1(x)$

$$i.e) f(x) = a f_1(x), g(x) = b. g_1(x)$$

$$\therefore f(x).g(x) = a.b.f_1(x) \cdot g_1(x)$$

$$\text{cont}(f(x).g(x)) = a.b \text{cont}(f_1(x).g_1(x))$$

$$= a.b.1 [ \text{since } f_1 \text{ and } g_1 \text{ are primitive} ]$$

$$= a.b$$

$$= \text{cont. } f(x). \text{cont. } g(x)$$

Theorem:

Let  $f(x)$  be an irreducible primitive polynomial in  $Z[x]$ , then  $f(x)$  is irreducible in  $Q[x]$ .

Proof:

Suppose that  $f(x)$  is primitive in  $Z[x]$  otherwise, there exist a primitive polynomial  $f(x) \in Z[x]$  s.t  $f(x) = \text{cont. } f(x) \cdot f_1(x)$   
 suppose that  $f(x)$  is reducible in  $Q[x]$  this means  $\exists h(x).g(x) \in Q[x]$  s.t  $f(x) = h(x).g(x)$  and  $\deg g(x) \geq 1$ ,  $\deg h(x) \geq 1$

$$\text{Now } g(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \cdots + \frac{a_m}{b_m}x^m$$

$$h(x) = \frac{c_0}{d_0} + \frac{c_1}{d_1}x + \cdots + \frac{c_l}{d_l}x^l$$

where  $a_0, \dots, a_m$ ,  $b_0, \dots, b_m$ ,  $c_0, \dots, c_l$ ,  $d_0, \dots, d_l \in Z$

Let  $b = g.c.d(b_0, \dots, b_m)$ ,  $d = g.c.d(d_0, \dots, d_l)$

$$b \cdot d (f(x)) = b \cdot g(x) \cdot d \cdot h(x)$$

$$g(x) = \text{cont } g(x) \cdot g_1(x) \text{ and } h(x) = \text{cont } h(x) \cdot h_1(x)$$

Where  $g_1(x)$  and  $h_1(x)$  are primitive

$$\rightarrow g(x) = b_1 \cdot g_1(x) \text{ and } h(x) = d_1 \cdot h_1(x)$$

$$\therefore bd \cdot f(x) = b_1 \cdot d_1 \cdot g_1(x) \cdot h_1(x)$$

$$\text{cont}(b \cdot d \cdot f(x)) = \text{cont}(b_1 \cdot d_1 \cdot g_1(x) \cdot h_1(x))$$

$$= b_1 \cdot d_1 \cdot \text{cont}(g_1(x) \cdot h_1(x)) = b_1 \cdot d_1$$

$$b \cdot d \cdot f(x) = b_1 \cdot d_1 \cdot g_1(x) \cdot h_1(x) = \text{cont}(b \cdot d \cdot f(x)) \cdot g_1(x) \cdot h_1(x)$$

$$= b \cdot d \cdot \text{cont}(f(x)) \cdot g_1(x) \cdot h_1(x)$$

$$= g_1(x) \cdot h_1(x) \in Z[x], [f(x) \text{ primitive by assumption}]$$



$f(x)$  is reducible in  $\mathbb{Z}[x] \rightarrow \mathbb{C}!$

Thus  $f(x)$  is irreducible in  $\mathbb{Q}[x]$

### Theorem:(Eisenstein)

Let  $f(x) = a_0 + a_1x + \cdots + a_nx^n$  be a polynomial in  $\mathbb{Z}[x]$  with positive degree if there exist a prime number  $p$  s.t  $p/a_i \quad \forall \quad 0 \leq i < n-1$  ,  $p \nmid a_n$  and  $p^2 \nmid a_0$ , then  $f(x)$  is irreducible in  $\mathbb{Q}[x]$ .

### Kronecker Theorem:

Let  $F$  be a field and  $f(x)$  be a non-constant polynomial in  $F[x]$  then there exists an extension field  $E$  ,  $\alpha \in E$  s.t  $f(\alpha) = 0$ .

### Proof:

$F$  is a field  $\rightarrow F$  is U.F.D [field  $\rightarrow$  E.D , E.D  $\rightarrow$  U.F.D ]

Let  $f(x) \in F[x]$ , then we can write  $f(x)$  as a product of irreducible polynomial :

$f(x) = p_1(x) \cdot p_2(x) \cdots p_n(x)$  where  $p_i(x)$  is irreducible  $\forall i = 1, \dots, n$

$\langle p_1(x) \rangle$  is maximal.

$\therefore \frac{F[x]}{\langle p_1(x) \rangle}$  is a field.

Put  $E = \frac{F[x]}{\langle p_1(x) \rangle}$

Define  $\phi = F \rightarrow \frac{F[x]}{\langle p_1(x) \rangle}$  by  $\phi(a) = a + \langle p_1(x) \rangle \quad \forall a \in F$

(1)  $\phi$  is well define :

$$\text{if } a = b \rightarrow a + \langle p_1(x) \rangle = b + \langle p_1(x) \rangle \rightarrow \phi(a) = \phi(b)$$

(2)  $\phi$  is well homomorphism?

$$\begin{aligned}\phi(a + b) &= a + b + \langle p_1(x) \rangle = a + \langle p_1(x) \rangle + b + \langle p_1(x) \rangle \\ &= \phi(a) + \phi(b)\end{aligned}$$

$$\begin{aligned}\phi(a \cdot b) &= a \cdot b + \langle p_1(x) \rangle = (a + \langle p_1(x) \rangle) \cdot (b + \langle p_1(x) \rangle) \\ &= \phi(a) \cdot \phi(b)\end{aligned}$$

(3)  $\phi$  is 1-1 :

If  $\phi(a) = \phi(b)$

$$a + \langle p_1(x) \rangle = b + \langle p_1(x) \rangle \leftrightarrow a - b \in \langle p_1(x) \rangle ,$$

$$\therefore a - b = 0 \rightarrow a = b .$$

$$F \subset E = \frac{F[x]}{\langle p_1(x) \rangle} , \quad \therefore E \text{ is extension for } F$$

Let  $\alpha \in E$  ,  $\alpha = x + \langle p_1(x) \rangle$  ,  $x \in F[X]$

To prove  $f(\alpha) = 0$  ?

$$f(\alpha) = p_1(\alpha) \cdot p_2(\alpha) \cdots p_n(\alpha)$$

$$\text{if } p_1(\alpha) = 0 \rightarrow f(\alpha) = 0$$

If  $\deg p_1(\alpha) \geq 1$  ,  $p_1(x) = a_0 + a_1x + \cdots + a_nx^n$

$$I = p_1(\alpha) = a_0 + a_1 \alpha + \cdots + a_n \alpha^n ,$$

$$p_1(x + \langle p_1(x) \rangle) = a_0 + a_1x + a_2x^2 \cdots + a_nx^n + \langle p_1(x) \rangle$$

$$= p_1(x) + \langle p_1(x) \rangle$$

$$= \langle p_1(x) \rangle = 0$$

$$\therefore p_1(\alpha) = 0 \rightarrow f(\alpha) = 0 .$$

H.W/

Let  $f(x) = x^2 + 1 \in R[x]$ ,  $\alpha = x + (x^2 + 1)$ , prove that  $\frac{R[x]}{\langle x^2 + 1 \rangle} \cong C$ .

Sol/ Define  $h: C \rightarrow \frac{R[x]}{\langle x^2 + 1 \rangle}$  by  $h(a + ib) = a + bx + \langle x^2 + 1 \rangle$

$$1) \quad h(a + ib) = h(c + id)$$

$$a + bx + \langle x^2 + 1 \rangle = c + dx + \langle x^2 + 1 \rangle$$

$$\rightarrow a + bx - c - dx \in \langle x^2 + 1 \rangle$$

$$\rightarrow a + bx - c - dx = 0 \rightarrow a - c = 0, \quad b - d = 0$$

$$\rightarrow a = c \quad \& \quad b = d \rightarrow a + ib = c + id, \quad \therefore 1 - 1$$

1)  $h$  is homomorphism

$$h(a + ib + c + id) = h(a + c + (b + d)i)$$

$$= a + c + (b + d)x + \langle x^2 + 1 \rangle = a + bx + \langle x^2 + 1 \rangle + c + dx + \langle x^2 + 1 \rangle$$

$$= h(a + ib) + h(c + id).$$

$$h(a + ib) \cdot h(c + id) = h(a + ib) \cdot h(c + id)$$

Example::

$$f(x) = x^4 - 4 \in Q[x]$$

$$f(x) = (x^2 - 2)(x^2 + 2)$$

Use Kronecker's Theorem,  $\alpha = x + \langle p_1(x) \rangle = x + \langle x^2 - 2 \rangle$

H.W//

1) let  $f(x) = x^2 + 5$  prove that  $\langle f(x) \rangle$  is irreducible in  $Z[x]$  (Hint:  $\phi: Z[x] \rightarrow Z[\sqrt{-5}]$ ,  $\phi(g(x)) = g(\sqrt{-5})$ )

2)  $f(x) = x^4 + x^2 + 1 \in Q[x]$ , is  $f$  irreducible and have a root in  $Q$ ?

3)  $f(x) = x^3 + \bar{3}$  is  $f(x)$  irreducible in  $Z_6$ ?

4) Use Eneshtin theorem to show that if:

a)  $f(x) = x^4 - 2x^3 + 6x^2 + 4x - 10 \in Z[x]$  [Hint:  $p = 2$ ]

b)  $f(x) = 1 + 5x + 10x^2 + 5x^3$

5) Prove that if  $f(x) = 1 + x + x^2$  is irreducible in  $Q[x]$  or not?

Remarks

- 1)  $f(x)$  is irreducible iff  $f(x + 1)$  is irreducible in  $Q$ .
- 2)  $f(x)$  is irreducible, iff  $f(x - 1)$  is irreducible in  $Q$ .
- 3) The polynomial  $f(x) = 1 + x + x^2 + \dots + x^{p-1}$  (where  $P$  is prime) is irreducible in  $Q[x]$ ?

Proof:

(1)&amp; (2) (H.W)

Proof: (3)

$$\begin{aligned}
 f(x + 1) &= 1 + (x + 1) + (x + 1)^2 + \dots + (x + 1)^{p-1} \\
 &= \frac{(x + 1)^p - 1}{(x + 1) - 1} = \frac{(x + 1)^p - 1}{x} \\
 &= \frac{1}{x} [(x + 1)^p - 1] \\
 &= \frac{1}{x} \left[ x^p + px^{p-1} + \frac{p(p-1)}{2!} x^{p-2} + \dots + px \right] \\
 &= \left[ x^{p-1} + px^{p-2} + \frac{p(p-1)}{2!} x^{p-3} + \dots + p \right].
 \end{aligned}$$

We choose  $p$  to satisfy the theorem,  $\therefore$  by Eisenstein theorem, then  $f(x + 1)$  is irreducible on  $Q[x]$  and by remark (1)  $f(x)$  is irreducible on  $Q[x]$ .

Defintion:

The field  $E$  is an extension to the field  $F$  if  $F$  is a subfield in  $E$ .

Example:

$R$  is an extension field of  $Q$ .

$C$  is an extension field of  $R$ .

$C$  is an extension field of  $Q$ .

H.W//

Let  $f(x) = x^4 - 5x^2 + 6 \in Q[x]$  find an extension field  $E$  to  $Q$  by using kronker theorem?

**Hint:**  $E = \frac{Q[x]}{\langle x^2 - 2 \rangle}$ ,  $\alpha = x + \langle x^2 - 2 \rangle$

H.W//

Let  $f(x) = x^2 + 5x + 8$ , is  $f(x)$  irreducible on  $Q$ ?

**Hint:**  $f(x + 1) = \dots$

Defintion:

Let  $E$  be an extension field of  $F$ , let  $\alpha \in E$  we called  $\alpha$  algebraic element if there exists a non zero polynomial  $f(x) \in F[x]$  s.t  $f(\alpha) = 0$ .

Otherwise we say that  $\alpha$  is transcendental element

Example:

$\mathcal{R}$  extension field to  $Q$

$\sqrt{2} \in R$  is  $\sqrt{2}$  algebraic element  $Q$ ?

Note that  $f(x) = x^2 - 2 \in Q[x]$  &  $f(\sqrt{2}) = 0$

$\therefore \sqrt{2}$  is algebraic element.

H.W// Is

1)  $\alpha = \sqrt{1 + \sqrt{3}} \in R$  algebraic on  $Q$ ?

2)  $\pi$  is algebraic on  $Q$ ?

3)  $e$  is algebraic on  $Q$ ?

**Sol:**  $(1)\alpha^2 = 1 + \sqrt{3} \rightarrow \alpha^2 - 1 = \sqrt{3} \rightarrow (\alpha^2 - 1)^2 = 3$

$$\alpha^4 - 2\alpha^2 - 1 = 3 \rightarrow \alpha^4 - 2\alpha^2 - 4 = 0 .$$

### Defintion::

Let  $R$  is I.D  $f(x) \in R[x]$  non-constant,  $f$  is irreducible if  $f \nmid h(x)$  ,  
 $k(x) \in R[x]$  s.t  $f(x) = h(x).k(x)$  ,  $\deg(h(x)) \geq 1, \deg(k(x)) \geq 1$

### Example:

$$f(x) = 2x^2 - 4 \in \mathbb{Z}[x],$$

$$f(x) = 2(x^2 - 2) = 2(x - \sqrt{2})(x + \sqrt{2})$$

$$\sqrt{2} \notin \mathbb{Z}$$

**Note:**  $f(x) = ax + b \in R[x]$  is irreducible

$$f(x) = h(x).k(x) \text{ since } \deg f(x) < \deg(h(x) \cdot k(x))$$

### Example:

$$f(x) = x^3 + 3x + 2 \in \mathbb{Z}_5[x]?$$

**Sol:** Claim that  $f$  is irreducible , if  $f$  not irreducible then

$f(x) = h(x) \cdot k(x)$  with  $\deg h, k > 0$  , then either  $k$  or  $h$  has a first order.

i. e)  $h(x) = x - a$  ,  $a \in \mathbb{Z}_5[x]$   $h(a) = a - a = 0$  and since

$$f(x) = h(x) \cdot k(x) = (x - a) \cdot k(x) \quad , \quad \therefore f(a) = (a - a) \cdot k(a) = 0$$

$\therefore f$  has a root in  $\mathbb{Z}_5[x]$  but  $f$  has no root in  $\mathbb{Z}_5[x]$  since

$$f(a) = 2 \quad , \quad f(1) = 1 \quad , \quad f(2) = 1 \quad , \quad f(3) = 3 \quad , \quad f(4) = 78 \quad \text{C! With}$$

$$f(x) = h(x) \cdot k(x) \quad \therefore f \text{ is irreducible.}$$

### Theorem:

Let  $F$  be a field and  $f(x) \in F[x]$ ,  $\deg f(x) = 2$  or  $3$ , then  $f$  is irreducible iff  $f(x)$  has no root in  $F$ .

Example:

$$f(x) = 2x^2 + 4 \in R[x]$$

$= 2(x^2 + 2) = 2(x - \sqrt{2}i)(x + \sqrt{2}i) \quad \therefore f$  has no root in  $R \quad \therefore f$  is irreducible

Example:

$$f(x) = x^3 + 3 \in Z_6[x].$$

$$f(0) = 3, \quad f(1) = 4, \quad f(2) = 5, \quad f(3) = 0$$

$\therefore f$  is not irreducible

Example(H.W)

$$f(x) = x^3 + x + 1 \in Z_5[x].$$

Example(H.W)

$$f(x) = x^2 + 3 \in Z_7[x].$$