The Rings (2)

The Fouth Class

By

Dr. Nuhad Salim Al-Mothafar

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.

(3

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) $(R,.)$. is a semigroup and

3) The operation . 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:$\bar{2}.\bar{3} = \bar{0}$, $\bar{3}.\bar{4} = \bar{0}$, $\bar{2},\bar{3},\bar{4}$ 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 $(R, +, .)$ is said to be ***field*** if $(R - \{0\}, .)$ 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 $\emptyset = S \subseteq R$, then $(S, +, \cdot)$ is called a ***subring*** if $(S, +, \cdot)$ is a ring itself.

Example:

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

Rrmark:

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) $a.b \in S \quad \forall a, b \in S.$

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) $a - b \in I \ \forall a, b \in I$.

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

Remark:

Every ideal is subring.

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

(1) $I \neq \emptyset$

(2) 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:

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

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

$\therefore Z$ is not ideal

Remark(*):

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 $a.b \in I \Rightarrow 1 \in I$

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

Definition:

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

Theorem:

$(Z, +, .)$ 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 Z_6 the ideals are:

$$\{0\}\ , Z_6\ , \{\bar{0}, \bar{3}\}, \{\bar{0}, \bar{2}, \bar{4}\}$$

$\{\bar{0}, \bar{3}\}$ is the maximal in Z_6.

$\{\bar{0}, \bar{2}, \bar{4}\}$ is the maximal in 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 fiald.

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)$4Z$is an ideal in Z, but not a prime ideal in Z.

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

3){0}is not a prime ideal in 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:

$Z_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ 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 Ibe an ideal of a ring R. Then the nil radical of I denoted by $\sqrt{I}$ is the set:

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

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 $\exists\ n \in Z^+ \ni w^n \in I \cap J$, 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 $x \in \sqrt{\sqrt{I}}$ $\exists$ $n \in Z^+ \ni x^n \in \sqrt{I}$, and then $\exists$ $m \in Z^+ \ni (x^n)^m \in I$, 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$\exists$ $n \in Z^+ \ni$ $x^n \in I$ and $\exists$ $m \in Z^+ \ni y^m \in J$.

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

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

Definition:

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

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

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

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

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 $w \in \sqrt{I} \, \exists$ $n \in Z^+ \ni w^n \in I$, 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 $6 = 2.3 \in \langle 6 \rangle$

Theorem:

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

Proof: ⇒)Let I be a semiprime ideal and let $a + I$ be a nilpotent element in $\frac{R}{N}$ ∃ 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 $a \in I \Leftrightarrow a + I = I$

⇐)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 $\frac{R}{N}$, 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 $k \in Z^+$.

Example: *In* Z. *Let* $I = 8Z$, $4.2 = 8 \in 8Z$, $4 \notin 8Z$ *and* $2^3 = 8 \in 8Z$, *so* $8Z$ *is* primary ideal.

Remark:

Every prime ideal is primary.

Q: Is the converse true?

$8Z$ is primary ideal but not prime since $4.2 = 8 \in 8Z$ $but\ 4 \notin 8Z\ and\ 2 \notin 8Z$

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 $\frac{R}{N}$, 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 $\exists\ k \in Z^{+} \ni a^{k} \in I \leftrightarrow a^{k} + I = I$ thus $(a + I)^{k} = I$ and $a + I$ is a nilpotent element.

$\Leftarrow$) Let $x \cdot y \in I$ and $x \notin I$, then $x \cdot y \in I \leftrightarrow x.y + I = I \leftrightarrow (x + I)(y + I) = I$, 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 $\frac{R}{N}$ $\exists\, n \in Z^{+} \ni (y + I)^{n} = I = y^{n} + I = I \Leftrightarrow y^{n} \in I$.

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 $1' \in f(M) \to 1' = f(m)$; $m \in M$. But $f(1) = 1' \to f(m) = f(1) \to f(m-1) = 0 \to m-1 \in \ker f \subseteq M$ $\to m-(m-1) \in M \to 1 \in M$ 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* $\to \exists\, x \in R \ni f(x) = y$, $x \notin M$.

Then by theorem (let M be a proper ideal of a ring R. If M is maximal ideal in R iff $< M, x > = R$, $x \notin M$) $< M, x > = R \to 1 = m + tx$; $m \in M$, $t \in R$, 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 $f^{-1}(w) = 1$; $w \in M' \to f(1) \in M' \to 1' \in M'$] . Let $f^{-1}(M') \subsetneq J \subseteq R$, then

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

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

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

$k + rx - 1 \in kerf \subseteq f^{-1}(M') \subseteq J$ 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 $n \in Z^+$.

$f(a.b) \in f(I)$ [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 $n \in Z^+$. Thus $f(b^n) \in f(I) \to (f(b))^n \in f(I)$ 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 $f^{-1}(K) = R$ [$1 \in f^{-1}(K) \Longrightarrow f(1) \in K \Longrightarrow 1_R \in K$ 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 $\exists n \in Z^+ \ni (f(y))^n \in K$, 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,$f(M) \neq R'$ [$1_{R'} \in f(M) \to 1_{R'} = f(m)$, $\exists n \in Z^+$ such that $f(m) = f(1)$, then $f(m-1) = 0$, then $(m-1) \in Kerf \subseteq M$, 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 $\exists n \in Z^+ \ni w^n \in f(M)$, 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 $(x^n - m) \in Kerf \subseteq M$, then $(x^n - m) \in M$ but $m \in M$, hence $x^n \in M$, then, $x \in \sqrt{M} = M \Longrightarrow x \in M$ [since M is semiprime and $\sqrt{M} = M$], then $f(x) \in f(M) \Longrightarrow w \in f(M)$, 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:

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

Example: (1) In Z, (2Z) ∩ (3Z) ∩ (7Z) ∩ … = {0}, J(Z)=0

(2) In Z_6, $\{\bar{0}, \bar{2}, \bar{4}\} \cap \{\bar{0}, \bar{3}\} = \{0\}$, $J(Z_6)=0$.

(3) Z_4, M = $\{\bar{0}, \bar{2}, \}$.

$\therefore J(Z_4) = \{\bar{0}, \bar{2}, \}$.

Remark:

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

Proof: Let $a, b \in J(R)$, then $a, b \in = \cap \{M: M is\ maximal\ ideal\ in\ R\}$, then $a, b \in M \ \forall\ maximal\ ideal\ M$, 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 $M = R$C!. Thus $1 + I$ has inverse.

$\Leftarrow$) suppose that each member of $1 + I$ has inverse, but $I \nsubseteq J(R) = \cap M\, ; M$ is maximal ideal, then $I \nsubseteq M$.

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 $< M, a > = R$, 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 $I =< a >$ by above lemma, we have $a \in < a > \subseteq J(R)$ if and only if $1 +< a >$ 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 $(*)$.

$a.[(1+(-1)a)b] = 0.b$, so $a.1 = 0$. 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 $\exists\, n \in Z^+ \; s.t \; a^n = 0$, 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 Z: L(Z)=∩(P)={0}, L(Z)=0, where P is prime.

(2) Find $L(Z_8)$, $L(Z_6)$, $L(Z_{12})$.(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 $r^n \notin I \ \forall \ n \in Z$, 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 $x \in \cup_{\alpha \in \Lambda} C_\alpha$, then $\exists \ \beta \in \Lambda \ s.t \ x \in C_\beta$, then $rx \in C_\beta$.since $\cup_{\alpha \in \Lambda} C_\alpha$ is an ideal in F.

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

3)$(\cup_{\alpha \in \Lambda} C_\alpha) \cap \boldsymbol{S} = \cup_{\alpha \in \Lambda} (C_\alpha \cap S) = \cup \ (\emptyset) = \emptyset$**.** Thus $\cup_{\alpha \in \Lambda} C_\alpha \in F$. 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 $\exists\, m,k \in Z^{+}\ s.t\ r^{m} \in \langle P,x\rangle,\ r^{k} \in \langle P,y\rangle$, then $r^{m+k} = r^{m}.r^{k} \in \langle P,x\rangle.\langle P,y\rangle \subseteq \langle P,x,y\rangle = P$.

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

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

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

Corollary:

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

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 ( ) $\exists\, n \in Z$ s.t $\left(x + L(R)\right)^{n} = L(R)$, then $x^{n} + L(R) = L(R)$, then $x^{n} \in L(R)$, then by ( ) $\exists\, n \in Z\ s.t\ (x^{n})^{m} = 0$, 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. $f\big(J(R)\big) = J(R')$.
2. $f^{-1}\big(J(R')\big) = J(R)$.

Proof:

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

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

Let $w \in f\big(J(R)\big)$, $w = f(x)$; $x \in J(R)$. 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 *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 *is homo.*] $\Rightarrow$

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

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

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

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] .

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

Since f is onto, $\exists\, r \in R$ $s.t$ $f(r) = r'$, $\exists\, t \in R$ $s.t$ $f(t) = z$, $f(1) = 1'$. $(1' + r'y).z = 1' \Rightarrow [f(1) + f(r).f(x)].f(t) = f(1) \Rightarrow f\big((1+rx).t\big) = f(1) \Rightarrow f\big((1+rx).t - 1\big) = 0 \Rightarrow (1+rx).t - 1 \in ker\, f \subseteq J(R)$. 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 $(t\,w)$ in R iff $x \in J(R)$, hence $J(R') \subseteq f\big(J(R)\big) \cdots (2)$.

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

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

Let $x \in f^{-1}\big(J(R')\big) \Rightarrow f(x) \in J(R') = f\big(J(R)\big)$, then $f(x) \in f\big(J(R)\big)$, 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 $f^{-1}\big(J(R')\big) \subseteq J(R) \cdots (1)$.

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

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

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

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

Theorem:

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

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

Proof:

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

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

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

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

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

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

Let $y \in L(R') \Rightarrow y^n = 0'\ n \in Z^+$, since f is onto $\Rightarrow \exists\, b \in R\ s.t\ f(b) = y$.
$0' = y^n = \big(f(b)\big)^n = f(b^n)$, since f is homo. $\Rightarrow b^n \in Kerf \subseteq L(R)$

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

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

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

Let $x \in f^{-1}\big(L(R')\big) \Rightarrow f(x) \in L(R') = f\big(L(R)\big)$, then $f(x) \in f\big(L(R)\big)$, then $\exists\, y \in L(R)\ s.t\ f(x) = f(y) \Rightarrow f(x-y) = 0$ $[f\ is\ homo.]$

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

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

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

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

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

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

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" $(a \setminus b)$ 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 $a.c \setminus b.c \ \forall c \in R$.
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 Z: $2, -2$.

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

(-1) has an inverse in 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 $Z(i)$.

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

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

$(a + ib).(c + id) = 1$, so $(a - ib).(c - id) = 1$, then

$$(a + ib).(c + id).(a - ib).(c - id) = 1$$

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

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

Or $a^2 = 1$, $b^2 = 0 \Rightarrow a = \pm 1$, $b = 0$. 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 $a \setminus b$ and $b \setminus a$.

3) $\langle a\rangle = \langle b\rangle$.

Proof:

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

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

$u_1u_2 = ba^{-1}ab^{-1} = bb^{-1} = 1 \Rightarrow u_1\,,u_2$ are invertible element. $\Rightarrow a\,,b$ are associated elements

Definition:

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

1) $d \setminus a_i \quad \forall\, i = 1,2,\cdots,n$.

2) If $c \setminus a_i \quad \forall\, i = 1,2,\cdots, n$ implies that $c \setminus d$.

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

Eexample:

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

Theorem:

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

***Proof*:** $\Rightarrow)$

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

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

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

$\Rightarrow \quad x = t_1a_1 + t_2a_2 +\cdots +t_n a_n \quad ; \quad t_i \in R \qquad \cdots (*)$

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

Put a_i in $(*)$.

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

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

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

$a_i \in \langle d\rangle \;\forall\, i = 1,2,\cdots, n \Rightarrow \exists\, b_i \in R \;s.t\; a_i = db_i \Rightarrow d \setminus a_i \quad \forall\, i = 1,2,\cdots, n$. Now, suppose that $\exists\, c \in R \quad s.t \quad c \setminus a_i \quad \forall\, i \Rightarrow \exists\, s_i \in R \;\; s.t \;\; a_i = s_i\, c \Rightarrow$

$$d = r_1a_1 + r_2a_2 + \cdots + r_n a_n$$

$$= r_1s_1 c + r_2s_2 c + \cdots + r_n s_n c$$

$$d = (r_1s_1 + r_2s_2 + \cdots + r_n s_n).c \Rightarrow c \setminus d$$

$\therefore$ d *is* $g.c.d(a_1, a_2, \cdots, a_n)$

Corollary:

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

In fact $g.c.d(a_1, a_2, \cdots, a_n) = r_1a_1 + r_2a_2 + \cdots + r_n a_n$ for suitable choice $r_1, r_1, \cdots, r_n \in R$.

Definition:

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

Theorem:

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

Proof:

Since a, c are relatively prime elements

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

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

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

Theorem:

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

Proof: $\Rightarrow$)

Let $c = l.c.m(a_1, a_2, \cdots, a_n)$, 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 $l.c.m(a_1, a_2, \cdots, a_n) \Rightarrow \quad a_i \setminus c \quad \forall\, i = 1,2,\cdots, n$

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

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

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

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

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

$\Rightarrow \ a_i \setminus k \quad \forall\, i$ but $c = l.c.m(a_1, a_2, \cdots, a_n)$,

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

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

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

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

$\Rightarrow\ a_i \setminus c \quad \ldots (1)$.

We suppose that $\exists\ \acute{c} \in R \quad s.t \quad a_i \setminus \acute{c} \quad \forall\, i$, we must prove that $c \setminus \acute{c}$.

$$a_i \setminus \acute{c} \Rightarrow \quad \acute{c} = r_i\ a_i \quad \forall\, i \quad r_i \in R \quad \Rightarrow \quad \acute{c} \in \langle a_i \rangle \quad \forall\, i\ .$$

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

$$\acute{c} = w.c \Rightarrow \quad c \setminus \acute{c} \quad \cdots (2)\ .$$

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

Corollary:

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

Proof:

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

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

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

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 $a \setminus c.b$, then either $a \setminus c$ or $a \setminus b$.

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 $\acute{p}$ is associated with p, then $\acute{p}$ 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. $(p')^{-1}.p' = (p')^{-1}.up \Rightarrow 1 = \left[(p')^{-1}.u\right].p \Rightarrow p$ is invertible C! [since p is prime element].
   c) If $p' \setminus c.b \Rightarrow c.b = t.p'$ $, t \in R \Rightarrow c.b = t.u.p \Rightarrow c.b = (t.u).p \Rightarrow p \setminus c.b$ but p is prime element, then either $p \setminus c.$ or $p \setminus b$ if $p \setminus b \Rightarrow b = r.p \Rightarrow b = (r.u').\Rightarrow p' \setminus b$. Similarly, if $p \setminus c \Rightarrow p'$ is prime element.
2) Since q, q' are associated, then $q' = uq$ where u has an inverse $\Rightarrow u^{-1}.q' = q \quad \cdots (*)$.
   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 $\Rightarrow (q')^{-1}.q' = (q')^{-1}.uq \Rightarrow 1 = \left[(q')^{-1}.u\right].q \Rightarrow q$ has inverse C! [since q is prime element].
   c) If $q' = c.b \Rightarrow u.q = c.b \Rightarrow q = (u^{-1}.b).c$ since q is irreducible element, then either c has an inverse or $u^{-1}.b$ has an inverse.
   If $u^{-1}.b$ has an inverse $\Rightarrow \exists\ w \in R\ \ s.t\ \ w(u^{-1}.b) = 1$
   $\Rightarrow (wu^{-1})\, b = 1$
   $\Rightarrow b$ has an inverse. Thus q' 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 $a, b \in R\ s.t\ p = a.b\ (1.p = a.b) \Rightarrow p \setminus a.b$, p is prime element , then either $p \setminus a$ or $p \setminus b$. if $p \setminus a \Rightarrow a = r.p\ , r \in R \Rightarrow a.b = (r.p).b \Rightarrow p = r.b.p \Rightarrow 1 = r.b$

$\Rightarrow b$ has an inverse.

Similarly if $p \setminus b \Rightarrow p$ 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 $p \setminus a.b \Rightarrow p = a.b\ ;\ c \in R\ \cdots (*)$.

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 $a \in \langle d \rangle \Rightarrow a \in \langle p \rangle \Rightarrow a = r.p\ ;\ r \in R \Rightarrow p \setminus a$.

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

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

$b = bat_1 + bpt_2$

$b = bct_1 + pbt_2$

$b = p(ct_1 + bt_2)$

$\Rightarrow p \setminus b$.

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 $\{I_n\}$; $n \in Z^+$ is any infinite sequence of ideals of R $s.t$ $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots$, then there exist $m \in Z^+$ $s.t$ $I_n = I_m$ for all $n > m$.

Proof:

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

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

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

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

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 $a \in \langle p \rangle \Rightarrow a = p.c$, $c \in R$.

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

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

$\therefore \langle a \rangle \neq R$ $C!$ [$since\ a$ 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, $\langle p \rangle \neq R$ [$since\ p$ has no inverse]

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

If $p \setminus a \Rightarrow a = pk_1 \;\; , \; k_1 \in R \;\Rightarrow a \in \langle p \rangle$

Or $p \setminus b \Rightarrow b = pk_2 \;\; , \; k_2 \in R \;\Rightarrow b \in \langle p \rangle$

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

$\Leftarrow$)

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

Let $p \setminus a.b \Rightarrow a.b = m.p \;\; , \; m \in R \Rightarrow a.b \in \langle p \rangle$ 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 $p \setminus a$ or $p \setminus b$

Lemma:(*)

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

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) .

$a \in \langle a \rangle \subset \langle P \rangle \Rightarrow a \in \langle P \rangle \Rightarrow a = m.p \;\; , \; m \in R \Rightarrow p \setminus a$.

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 π on $\{1,2, \dots , n\}$ $s.t$ p_i , q_j are associated elements.

Example:

Z is UFD.

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

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 $a = p_1 . p_2 \dots p_n$ by theorem ( ) p_i is irreducible elements $\forall i$. Now suppose that $a = p_1 . p_2 \dots p_n = q_1 . q_2 \dots q_m$

Now we must show that $n = m$.

Suppose that $n < m$.

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

p_1 and q_1 are prime element in R and

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

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

We continue with these steps to $(n-1)$ times $\Rightarrow 1 = (u_1.u_2 \dots u_n).q_{n+1} \dots q_m \;\Rightarrow\; q_{n+1}, \dots, q_m$ has an inverse in R.

$\therefore\ n = m$

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

q_j, q_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

$p \setminus a \cdot b \;\Rightarrow\; a \cdot b = c \cdot p \;\cdots (1)$

1) If b has inverse

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

2) If a has inverse

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

3) If c has inverse

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

4) If a, b, c have no inverse

R is UFD $\Rightarrow\; a = p_1.p_2 \dots p_n \;,\; b = q_1.q_2 \dots q_m \;,\; c = k_1.k_2 \dots k_r$.

Where p_i, q_j, k_l are irreducible elements

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

Subdued in (1).

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

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

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

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

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

$\Rightarrow$ $p \setminus a$

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

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

$\Rightarrow$ $p \setminus b$

$\Rightarrow$ p is prime number.

Euclidian Domain(E.D)

Definition:

Let R be an I.D, then we say that R is E.D if there exists $\delta: R \to Z^+ \cup \{0\}$ satisfy the following:

(1) $\delta(a) = 0 \iff a = 0$
(2) $\delta(a.b) = \delta(a).\delta(b)$ $\forall a, b \in R$
(3) $\forall a, b \in R$ $s.t$ $b \neq 0$,$\exists$ $r, q \in R$ $s.t$ $a = qb + r$; $\delta(r) < \delta(b)$

Remark:

Every field is ED.

Proof:

Let F be a field, then $\forall$ $a \in F$, $a \neq 0$, $\exists$ $a^{-1} \in F$ $s.t$ $a.a^{-1} = 1$
Define $\delta: F \to Z^+ \cup \{0\}$ by:

$\delta(a) = 0$ if $a = 0$

$= 1 \quad if \quad a \neq 0$

(1) $\delta(a) = 0 \quad iff \quad a = 0 \quad (from\ def.)$

(2) $\delta(a.b) = 1 = 1.1 \quad = \delta(a).\delta(b)$

Let $a, b \in R \ , \ b \neq 0 \ \exists \ b^{-1} \in F \quad s.t \ b.b^{-1} = 1$

$a = (a.b^{-1}).b + 0 = qb + r.$

$\delta(r) = \delta(0) = 0 < \delta(b) = 1$.

$\therefore F$ is ED.

Theorem:

Let R be a P I.D, and let $0 \neq a \in R$ and a has no invers. Then a can be factorized to a finite number of irreducible elements

Proof:

Since $0 \neq a \ \exists$ a prim element $p_i \quad s.t \quad p_i \setminus a$.

$\Rightarrow \ a = t.\, p_1 \quad , \quad t \in R \qquad \cdots (*)$

$\Rightarrow \ a \in \langle a \rangle \ \Rightarrow \ \langle a \rangle \subset \langle t \rangle$. Notice that $\langle t \rangle \not\subset \langle a \rangle$ since if $\langle t \rangle \subset \langle a \rangle \ , \ t \in \langle t \rangle \Rightarrow t \in \langle a \rangle \Rightarrow \ t = s.a \ , \ s \in R$.

$\Rightarrow \ a = s.a.\, p_1 \ \Rightarrow \ 1 = s.\, p_1 \ \Rightarrow \ p_1$ is invertible C! since p_1 is prim element.

$\therefore \ \langle t \rangle \not\subset \langle a \rangle \quad i.e \quad \langle a \rangle \subsetneq \langle t \rangle$.

If t has an inverse $\Rightarrow \langle t \rangle = R$.

$1 \in R \Rightarrow 1 \in \langle t \rangle$ and $a \in \langle t \rangle \Rightarrow a = p_1 .t \Rightarrow a = p_1.1.t_1 \ , t_1 \in R$.

$\Rightarrow a = t_1.\, p_1 \quad C! \quad \Rightarrow t$ has no inverse.

By Lemma (*)(*) $\exists$ a prim element $p_2 \quad s.t \quad p_2 \setminus t \Rightarrow t = p_2 .\, t_2 \ , \ t_2 \in R$. $\Rightarrow \langle t \rangle \subsetneq \langle t_1 \rangle$ [in the similar way].

$i.e \quad \langle a \rangle \subsetneq \langle t \rangle \subsetneq \langle t_1 \rangle.$

We continue with this process until have the following ascending chain $\langle a \rangle \subsetneq \langle t \rangle \subsetneq \langle t_1 \rangle \subsetneq \cdots \subsetneq \langle t_n \rangle$.

Lemma (*)(*) this chain must stop $i.e \ \exists \ n \in Z^+ \ s.t$ the element has an inverse.

$\langle a \rangle \subsetneq \langle t \rangle \subsetneq \langle t_1 \rangle \subsetneq \cdots \subsetneq \langle t_n \rangle = R \Rightarrow a = p_1 . p_2 \ldots p_n . t_n \Rightarrow a = p_1 . p_2 \ldots p_n'$ where p_n' is associated with p_n. R is P I.D and p_n is irreducible element $\Rightarrow p_n'$ is irreducible element.

Example: Z is ED.

Define $\delta : Z \to Z^+ \cup \{0\}$ .by

$\delta(a) = |a| \quad \forall \ a \in Z$

(1)If $\delta(a) = 0 \Rightarrow |a| = 0 \Rightarrow a = 0$

If $a = 0 \Rightarrow \delta(0) = |0| = 0$.

(2) $\forall a, b \in Z$, $\delta(a.b) = |a.b| = |a|.|b| = \delta(a).\delta(b)$

(3)Let $a, b \in Z$, $b \neq 0$ from division algorithm we get

$\exists \ r, q \in Z \quad s.t \quad a = bq + r$.

$\delta(r) < \delta(b)$, $|r| < |b|$.

$\therefore Z$ is ED.

Theorem:

Let R be ED. with valuation δ .

(1) $\delta(1) = 1$

(2) $\forall \ a \neq 0, \ a \in R \ a$ .has an inverse $iff \ \delta(a) = 1$.

(3) $\forall a, b \in R$ are associated, then $\delta(a) = \delta(b)$.

Proof:

(1) Let $0 \neq a \in R$, $\delta(a) = \delta(a.1) = \delta(a).\delta(1) \Rightarrow 1 = \delta(1)$

(2) $\Rightarrow$) Let $0 \neq a \in R$ has an inverse $\Rightarrow \exists\ b \in R\ s.t\ a.b = 1$,
by (1) $\delta(1) = 1 \Rightarrow 1 = \delta(1) = \delta(a.b) = \delta(a).\delta(b)$.
$\Rightarrow \delta(a).\delta(b) = 1 \Rightarrow \delta(a) = \delta(b) = 1 \Rightarrow \delta(a) = 1$.

$\Leftarrow$)Suppose that $\delta(a) = 1 \Rightarrow 0 \neq a$ [R is ED $\delta(a) = 0\ iff\ a = 0$]

$1, a \in R$ by definition of E.D (3) $\exists\ r, q \in R \in s.t\ 1 = aq + r$ and $\delta(r) < \delta(b) = 1$.

$\therefore \delta(r) = 0\ iff\ r = 0 \Rightarrow 1 = a.q \Rightarrow a$ has an inverse.

(3) .Let $a, b \in R$ such that a, b are associated elements.
$\Rightarrow \exists\ u \in R$, u is invertible $s.t\ a = u.b \Rightarrow \delta(a) = \delta(u.b) = \delta(u).\delta(b) \Rightarrow 1.\delta(b) = \delta(b)$.

Remark:

(1) We denote to E.D some times by (R, δ).

(2) $r, q \in R$ from the definition of E.D called r: reminder and q: divisor(quotient).

Theorem:

Let (R, δ) be E.D, then r, q are unique iff $\delta(a + b) \leq \max\{\delta(a), \delta(b)\}$

$\forall\ a, b \in R$.

Proof:

$\Rightarrow$) Suppose that r, q are unique and $a, b \in R\ \ s.t$

$\delta(a + b) > \max\{\delta(a), \delta(b)\}$.

Notice that

$a = 1.(a+b) + (-b)\ \ s.t\ \ \delta(b) = \delta(-b) < \delta(a+b)$ since $b, -b$ associative

$a = 0.(a+b) + a \Rightarrow r, q$ are not unique C! .

$\therefore\ \delta(a+b) \leq \max\{\delta(a), \delta(b)\}$.

$\Leftarrow$)Let $a, b \in R\ \ s.t\ \ a = bq_1 + r_1\ \ and\ \ a = bq_2 + r_2$,

$\delta(r_1) < \delta(b)\ ,\ \delta(r_2) < \delta(b)$.

$\Rightarrow\ bq_1 + r_1 = bq_2 + r_2 \Rightarrow bq_1 - bq_2 = r_2 - r_1$

$\Rightarrow b(q_1 - q_2) = r_2 - r_1$.

$\Rightarrow \delta(b(q_1 - q_2)) = \delta(r_2 - r_1)\qquad \cdots (*)$.

$\Rightarrow (b).\delta(q_1 - q_2) = \delta(r_2 - r_1)$.

$\leq \max\{\delta(r_2), \delta(r_1)\} = \max\{\delta(r_2), \delta(r_1)\}$

$\Rightarrow \delta(b).\delta(q_1 - q_2) \leq \max\{\delta(r_2), \delta(r_1)\} < \delta(b)$

$\therefore\ \delta(q_1 - q_2) < 1 \Rightarrow \delta(q_1 - q_2) = 0$.

$\delta(q_1 - q_2) = 0\ \ iff\ q_1 - q_2 = 0 \Rightarrow q_1 = q_2$.

Sub. In $(*)$ $\ b.0 = r_2 - r_1 \Rightarrow r_2 = r_1$.

$\therefore\ r, q$ are unique.

Theorem:

Let (R, δ) be an E.D, then R is P.I.D.

***Proof*:**

Let I be an ideal in R. If $I = \langle 0 \rangle \Rightarrow I$ is P.I.D.

If $I \neq \langle 0 \rangle$, we take the set $S = \{\delta(a) : 0 \neq a \in I\} \neq \emptyset$, by the well ordered, then S is contain a smallest element say $\delta(a)$, we claim that

$I = \langle a \rangle \Rightarrow a \in I \Rightarrow \langle a \rangle \subseteq I$. Let $w \in I$ since R is E.D., $a, w \in I \Rightarrow \exists\ r, q \in R \quad s.t \quad w = aq + r\ ; \quad \delta(r) < \delta(a)$

$\Rightarrow 0 \neq r = w - aq \in I\ C!$

Since $\delta(a)$ is the smallest element in S and $\delta(r) < \delta(a)$.

$\therefore\ r = 0 \Rightarrow w = aq \Rightarrow w \in \langle a \rangle$.

$\therefore\ I \subseteq \langle a \rangle \Rightarrow I = \langle a \rangle$.

$\therefore\ I$ is P.I.D.

Remark:

Every E.D is U.F.D.

Proof:

Every E.D is P.I.D and every P.I.D is U.F.D.

Rings of polynomials:

Definition:

Let R be a ring, then the function $f: Z^+ \cup \{0\} \to R$ 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 nth term (or general term)for the sequence $\langle r_n \rangle$.

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

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, … ,0, …)

(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:

$\alpha + \beta = (a_1, a_2, a_3, \dots, a_n, 0, \dots) + (b_1, b_2, b_3, \dots, b_n, 0, \dots)$.

$= (a_1 + b_1, a_2 + b_2 \dots, a_n + b_n, 0, \dots)$.

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

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

Theorem:

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

Proof:

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

Define $\emptyset : R \to R\,[x]$ by $\emptyset(r) = (r, 0,0, \dots)\ \forall r \in R$.

1. $\emptyset$ is homomorphism:

$\emptyset(r_1 + r_2) = (r_1 + r_2, 0,0, \dots) = (r_1, 0,0, \dots) + (r_2, 0,0, \dots) = \emptyset(r_1) + \emptyset(r_2)$

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

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

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

3. $\emptyset$ is onto:

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

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

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

$\vdots$

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

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

Remark:

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

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

$(a_0, a_1, \dots, a_n, 0, \dots) = (a_0, 0, \dots) + (0, a_1, 0, \dots) + (0,0, \dots, a_n, 0, \dots)$

$= (a_0, 0, \dots) + (0, a_1, 0, \dots) \cdot (0,1,0, \dots)x + (0,0, a_2, 0, \dots) \cdot (0,0,1,0, \dots)x^2 + \cdots + (0,0, \dots, a_n, 0, \dots)(0,0, \dots, 1,0, \dots)x^n$

$= a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$

Definition:

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

Examples:

$\alpha(x) = 5 - x + x^3 - x^5 \in R[x]$

$= (5, -1,0,1,0, -1,0,0, \dots)$

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

Remark:

If $\alpha(x) = 0 \in Z[x]$, $\deg(\alpha) = 0$,then α 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 $\deg(\alpha(x) \cdot \beta(x)) = n \cdot m = \deg(\alpha(x)) + \deg(\beta(x))$.

Definition:

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

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

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

$$f(x) \cdot g(x) = a_0b_0 + (a_0b_1 + b_0a_1)x + (a_0b_2 + a_1b_1 + a_2b_1)x^2 + \cdots + a_nb_mx^{n+m}$$

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

$$= b_0a_0 + \cdots + b_ma_nx^{n+m} = g(x) \cdot f(x)$$

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 $R[x]$.

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

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

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

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

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

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

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

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

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

Remark:(3)

Let R be a commutative ring with one and let α , β be a non zero polynomial in $R[x]$, then $\deg\big(\alpha(x) + \beta(x)\big) \leq max(\deg \alpha(x), \deg \beta(x))$ or $\alpha(x) + \beta(x) = 0$.

Example:

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

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

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

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

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

Remark:(4)

$\deg\big(\alpha(x) \cdot \beta(x)\big) \leq (\deg \alpha(x) + \deg \beta(x))$ or $\alpha(x) \cdot \beta(x) = 0$.

Example:

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

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

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

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

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

Remark:(5)

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

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 $q(x), r(x) \in R[x]$ $s.t$

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

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

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

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

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

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

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

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

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

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

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

Suppose that the theorem is true for all polynomial.

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

$f(x) = a_0 + a_1 x + \cdots a_n x^n \;\; , \;\; a_n \neq 0$

$g(x) = b_0 + b_1 x + \cdots b_m x^m \;\; , \;\; b_m \;\neq 0 \,.$

Put $f_1(x) = f(x) - (a_n b_m^{-1}) \, x^{n-m} \cdot g(x) \qquad \ldots \quad (1)$

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

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

$f_1(x) = g(x).q_1(x) + r(x) \qquad \ldots \qquad (2)$

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

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

$g(x).q_1(x) + r(x) = f(x) - (a_n b_m^{-1}) \,.\, x^{n-m}.g(x)$

$f(x) = (q_1(x) + \; a_n b_m^{-1} \,.\, x^{n-m}).g(x) + r(x)$

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

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

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

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

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

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

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

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

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

$\max\{\deg\big(r(x)\big), deg(r_1(x))\} \geq \deg\big(g(x)\big) + deg\big(q(x) - q_1(x)\big)\ C!$
With $\deg\big(r(x)\big) < \deg\big(g(x)\big)$ and $deg(r_1(x)) < \deg\big(g(x)\big)$.

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

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

$\therefore q$ *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 $\acute{R}$ is called extension for R if $\acute{R}$ contain R as a subring ($R \subset \acute{R}$)

Theorem:

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

$f(x) = a_0 + a_1 x + \cdots + a_n x^n, a_n \neq 0$ and let $r \in cent\ R$, then $\exists$ a ring homomorphism.

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

$$f(r) = a_0 + a_1 r + \cdots + a_n r^n \in R$$

Proof:

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \quad , \quad a_n \neq 0$$

$$g(x) = b_0 + b_1 x + \cdots + b_m x^m \quad , \; b_m \neq 0 \quad n > m$$

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

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

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

$$\varphi_r\big(f(x).g(x)\big) = \varphi_r[(a_0 b_0) + (a_0 b_1 + a_1 b_0)x + \cdots + a_n b_m x^{n+m}]$$

$$= (a_0 b_0) + (a_0 b_1 + a_1 b_0)r + \cdots + a_n b_m r^{n+m}$$

$$= f(r).g(r)$$

$\therefore \;\; \varphi_r$ is a ring homomorphism.

Definition:

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

$$\varphi_r = \varphi_r(R[x]) = \{f(r) : f(r) \in \acute{R} \;\; s.t\ f(x) \in R[x]\}$$

Exampls:

1. In $(Z , +, \cdot)$.
   $f(x) = 1 + 2x \quad , \quad , \quad g(x) = 2 + 3x + 4x^2$
   $\deg(f.g) = 2 + 1 = 3 \quad [since\ a_n . b_m \neq 0\ ]$
2. In $(Z_n, + , \cdot)$.
   $f(x) = \bar{1} + \bar{3}x + \bar{2}x^2 \quad , \quad , \quad g(x) = \bar{5} + \bar{6}x + \bar{4}x^2 + \bar{6}x^3$
   $\deg(f.g) = \bar{5}$ false
   $[\ since\ a_n = \bar{2}\ , b_m = \bar{6}\ , \ a_n . b_m = \bar{2}.\bar{6} = 12 = \bar{0}\ ]$
   $\therefore \ \deg(f.g) = \bar{4}$

Lemma:

Let R be a commutative ring with 1 $f(x) = a_0 + a_1 x + \cdots + a_n x^n$,
, $g(x) = b_0 + b_1 x + \cdots + b_m x^m$ $s.t$ b_m has inverse, then
$\deg(f.g) = \deg(f) + \deg(g)$, $a_n \neq 0$, $b_m \neq 0$

Proof:

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

Exampl:

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

5 invertible.

(Division Algorithm)

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

Exampls:

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

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

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 $Z[x]$.

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

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 algorthim (for $f(x)$ and $x - a$) $\exists$ unique $r(x), q(x) \in R[x]$ $s.t$ $f(x) = (x - a)q(x) + r(x)$ ... (1)

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

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

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: $\Longrightarrow$)

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

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

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

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

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

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 of roots in R .

Proof:

By induction on $deg\big(f(x)\big)$ if $deg\ f(x)=0\rightarrow\ f(x)=c\ ,\ 0\neq c\in R$

$\rightarrow\ f$ has no root.

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

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 $deg\big(f(x)\big)=n$. (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. $\rightarrow (x-a)/f(x)\rightarrow f(x)=(x-a)q(x)\,;\ q(x)\in R[x]$.

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

$=deg(x-a)+deg(q(x))$ [since R is I.D]

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

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

∴ $f(x)$ 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

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

Proof:

Let $h(x) = f(x) - g(x)$, $deg\big(h(x)\big) \leq n$

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

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

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

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

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

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 $\rightarrow \quad f(x) = 0 \quad \forall\ x$.

Theorem:

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

Proof:

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

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

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

(1) $\delta(f(x)) = 0 \; if \; f(x) = 0$

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

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

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

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

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

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

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

$\because \; \deg\big(r(x)\big) < \deg(g(x))$.

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

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

$\therefore \; F[x]$ is E.D.

Corollary:

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

Proof:

F is a field $\to F[x]$ is E.D. $\to$ $F[x]$ 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 $\to$ $F[x]$ is E.D. $\to$ $F[x]$ is P.I.D. $\to$ $F[x]$ 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 polynomial $h(x), k(x) \in R[x]$ $s.t$ $g(x) = h(x).k(x)$ and satisfies that $h(x)$, $k(x)$ with positive degree not equal zero.

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

Example::

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

Remark(1):

(1)The reducible polynomial must it's 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] , b $\neq$ 0

but ax + b $\notin$ < x >

$\therefore$ < x > $\neq$ Z[x] .

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

φ is onto and homomorphism?

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

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

$= \{f(x) \in Z[x] : f(0) = 0\} = < x >$

$\therefore \frac{Z[x]}{<x>} \cong Z$ but Z is I.D then by [theorem]

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

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

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

$\to \therefore \frac{Z[x]}{<x>}$ is a field $\to$ 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 $\to$ by the last theorem Z is a field C!

Theorem:

Let F be afield, then the following are equivalent:-

(1) $f(x)$ is irreducible polynomial in $F[x]$.

(2) $f(x)$ is irreducible element in $F[x]$.

(3) $f(x)$ is prime element in $F[x]$.

Proof:

1 → 2) Suppose that $f(x)$ is irreducible polynomial in $F[x]$ and $f(x)$ has no inverse (?)

Suppose that $f(x) = g(x) . h(x)$

T.P either $g(x)$ or $h(x)$ has inverse

$\because f(x)$ is irreducible Polynomial $\rightarrow$ either $deg(h(x)) = 0.$

Or $deg(g(x)) = 0$

$\rightarrow$ either $h(x) = c_1$ *or* $g(x) = c_2$; $c_1, c_2 \in F$

Put F is a field $\rightarrow$ either c_1 or c_2 has an inverse i.e either $g(x)$ or $h(x)$ has an in inverse

$\rightarrow$ $f(x)$ is irreducible element

Proof: $2 \rightarrow 1$)

Let $f(x)$ be an irreducible element we want to prove that $f(x)$ is irreducible polynomial

$f(x) \neq 0 \rightarrow f(x)$ is not constant. $\rightarrow f(x)$ has no inverse

If we suppose that $f(x)$ is reducible polynomial.

Thus $\exists\ g(x), h(x) \in F[x]\ s.t\ f(x) = g(x). h(x)$

And each of $g(x)$, $h(x)$ are with positive degree

$i.e)\ deg\left(g(x)\right) \geq 1 \quad and \quad \deg\left(h(x)\right) \geq 1$

But $f(x)$ is irreducible element.

$\rightarrow$ either $h(x)$ has an invers $\rightarrow$ $h(x) = c_1$

$or\ g(x)$ has an inverse $\rightarrow$ $g(x) = c_2$

$\rightarrow$ $\deg(g(x))$ or $\deg(h(x)) = 0$ $C!$

$2 \rightarrow 3$)

$\because F$ is a field $\rightarrow F[x]$ $E.D$ $[Th.]$. $\therefore$ $F[x]$ $P.I.D$

$\rightarrow$) $\because$ $f(x)$ is irreducible $\rightarrow f(x)$ is prime

$\leftarrow$) $\therefore$ $f(x)$ is prime $\rightarrow f(x)$ is irreducible

Theorem [$if\ R\ is\ P.I.D\ then\ p\ is\ prime\ iff\ P\ is\ irr$educible].

(H.W):-

1- Prove that $f(x) = x^2 - 2 \in Q[x]$ is irreducible polynomial.

2- $f(x) = x^3 + x + 2 \in Z_{12}[x]$. Is $f(x)$ irreducible in $Z_{12}[x]$?

Theorem:

Let F be a field and $f(x)$ be a polynomial with $\deg f(x) =$ $2\ or\ 3\ in\ F[x], then\ f(x)\ is\ irreducible\ in\ F[x]\ iff\ f(x)$ has no root in F

Proof : $\rightarrow$) $Let\ f(x)\ be\ irr$educible in $F[x]$ and suppose that $f(x)$ has a root in $F[x]\ say\ c \rightarrow (x-c)/f(x)$ $[Th.]$

$\rightarrow$ $f(x) = (x-c) \cdot g(x)$

But F is a field $\rightarrow F\ is\ I.D.$

$\therefore \deg f(x) = \deg(x-c) + \deg(g(x))$

2	1	1
3	1	2

$\therefore f(x)$ is not irreducible. since $\deg(g(x)) \geq 1$ $\deg(x-c) = 1$ $C!$

$\therefore f(x)$ has no root in F

$\leftarrow$) Suppose that $f(x)$ has no root in F if $f(x)$ is not irreducible (reducible) thus $\exists\ h(x)\,,\ g(x)\ \in F\,[x]\ s.t$

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

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

2	1	1
3	1	2

$\rightarrow g(X)\ ,\ h(x)\ with\ \deg 1$

If $deg(g(x)) = 1 \rightarrow\ g(x) = ax + b$ the root of $g(x)$ is $-a^{-1}b$ (by assumption)

$g(-a^{-1}b) = a(-a^{-1})b + b = 0$

$\because f(x) = g(x).h(x)$

$f(-a^{-1}b) = g(-a^{-1}b) \cdot h(-a^{-1}b)$

$= 0 - h(-a^{-1}b) = 0$

$\therefore f(x)\ has\ a\ root\ C!$

$\therefore f(x)\ is\ irreducible. in\ F[x]$

Remark:

The last theorem is not true if $deg f(x) > 3$.

Example:(H.W)

Let $f(x) = x^4 + x^2 + 1\ \in Q(x)$. Is $f(x)$ irreducible. or not ?

Example:

$f(x)=x^5+x+1 \in Z_5[x]$?

Example:

$f(x)=x^3+3 \quad \in Z_6[x]$ is irreducible or not?

Theorem::

If R is I.D and $R[x]$ is P.I.D, then R is a field.

Proof::

Let $0 \neq a \in R$, $< x, a >$ is an ideal in $R[x]$.

$R[x]$ is $P.I.D$, then $< x, a > = < f(x) >$; $f(x) \in R[x]$.

$a \in < x, a > = < f(x) >$.

$\therefore a \in < f(x) > \rightarrow a = f(x) \cdot g(x)$; $g(x) \in R[x]$.

$x \in < x, a > \rightarrow x \in < f(x) > \rightarrow \exists\, h(x) \in R[x]$ $s.t$ $x = f(x) \cdot h(x)$

$0 = \deg a = deg f(x) + \deg(g(x))$

$\therefore deg(g(x)) = deg(f(x)) = 0 \rightarrow f(x) = a_0$

$= deg\,(x\,) = deg(f(x)) + deg\,(h(x))$

$\therefore 1 = \deg(h(x)$

$\therefore h(x) = a_1 x + b_1$; $f(x) = a_0$

$\therefore x = f(x) \cdot h(x) = a_0(a_1 x + b_1)$.

$\therefore x = a_0 a_1 x + a_0 b_1$, $\therefore a_0 a_1 = 1$

$\therefore a_0$ has an inverse

$< f(x)) > = < 1 > \rightarrow < x, a > = < 1 >$.

$\therefore 1 = x\, h_1(x) + a h_2(x)$; $h_1(x)$, $h_2(x) \in R[x]$.

$deg\ (1) = 0$

$\therefore \deg(h_1\ (x)) = 0$, $\deg\ h_2(x) = 0$.

$\therefore\ h_2(x) = b$, $\therefore\ a \cdot b = 1$ $(\ why?\ )$, $\therefore a$ has an inverse

Theorem: *(The Fundamental Theorem of Algebra)*

Let C be the field of complex numbers if $f(x) \in C[x]$ be a polynomial of positive degree, then $f(x)$ has at least one root in C .

Corollary(1):

If $f(x) \in C[x]$ with positive degree n, then $f(x)$ can be expressed in $C[x]$ as a product of n linear factor (not necessary distinct).

proof::

Let $deg\ f(x) = n$, by fund. Th of Algebra $f(x)$ has at least one root say c .

$\therefore (x - c)/f(x) \rightarrow f(x) = (x - c)f_1(x)$, $f_1(x) \in C[x]$, $\therefore deg f_1(x)$ is positive [since $\deg\big(f(x)\big) = deg(x - c) + \deg\big(f_1(x)\big)$]

By Fundamental Theorem of Algebra $f_1(x)$ has at least one root say c_2

$\therefore\ (x - c_2)/\ f_1(x) \rightarrow f_1(x) = (x - c_2) \cdot f_2(x)$

$\therefore\ f(\mathrm{x}) = (x - c_1\ )(x - c_2)f_2(x)$

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

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

$\overline{c_j} = a_j - ib_j$.

Now, $(x - c_j)(x - \overline{c_j}) = [x - (a_j + ib_j)][x - (a_j - ib_j)]$

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

Example:

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

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 $< f(x) >$ is a maximal or prime ideal in $F[x]$.

(3)The qoutient ring $\frac{F[x]}{<f(x)>}$ is a field

Proof:(H.W)

Example:

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

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

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

$\because$ C $field$ $\rightarrow$ $\frac{R[x]}{<x^2+1>}$ is $field$ iff $<x^2+1>$ 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

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

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

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

Example:

$4x^3 - 32x^2 - 16$, $contf(x) = g.c.d\ (4, -32, -16) = 4$

Example:

$f(x) = 3x^5 - 5x^2 + 7x + 1$, $contf(x) = 1$.

$\therefore$ $f(x)$ 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 $f_1(x) \in Z[x]$ $s.t$ $f(x) = cont\ f(x) \cdot f_1(x)$.

(3)If $f(x) \in Z[x]$ with positive degree, then $f(x) = cont\ (f(x)) \cdot f_1(x)$ 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 $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$, $a_n \neq 0$ and

$g(x) = b_0 + b_1x + \cdots + b_mx^m \in R[x]$, $b_m \neq 0$. 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 $p \nmid a_l$ ... (2).

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

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

$$c_{k+l} = \sum_{i+j} a_ib_j$$

$$= a_ob_{k+l} + a_1b_{k+l-1} + \cdots + a_{k-1}b_{l+1} + a_kb_l + a_{k+1}b_{l-1} + \cdots + a_{k+l}b_0$$

For choice of k and l $p \setminus a_{k+1}\, b_{l-1} + \cdots + a_{k+1}b_0$ and $p \setminus c_{k+l} \rightarrow p \setminus a_k\, b_l$ but p is prime number $\therefore\ p \setminus a_k$ or $p \setminus b_l$ $C!$ 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 $cont\big(f(x).g(x)\big) = cont\ f(x).cont\ g(x)$

Proof:

In case f and g are both primitive polynomial.

$\therefore cont.\big(f(x).g(x)\big) = 1$, , $\therefore cont.\big(f(x)\big) = 1$ and cont. (g(x))=1

$\therefore cont.\big(f(x).g(x)\big) = 1 = 1.1 = cont\big(f(x)\big).cont(g(x))$.

Now suppose that f and g are not primitive.

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

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

$i.e)\ f(x) = af_1(x), g(x) = b.g_1(x)$

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

$cont\ \big(f(x).g(x)\big) = a.b\ cont\big(f_1(x).g_1(x)\big)$

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

$= a.b$

$= cont.f(x).cont.g(x)$

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 $f(x) \in Z[x]$ $s.t$ $f(x) = cont.f(x).f_1(x)$

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 $deg\ g(x) \geq 1$, $\deg h(x) \geq 1$

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

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

$g(x) = cont\ g(x).g_1(x)$ and $h(x) = cont\ h(x).h_1(x)$

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

$\to g(x) = b_1.g_1(x)$ and $h(x) = d_1 \cdot h_1(x)$

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

$cont\ (b.d \cdot f(x)) = cont\ (b_1 \cdot d_1 \cdot g_1(x) \cdot h_1(x)\ )$

$= b_1 \cdot d_1 \cdot cont\left(g_1(x).h_1(x)\right) = b_1 \cdot d_1$

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

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

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

$f(x)$ is reducible in $Z\ [x]$ $C!$

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

Theorem: (Eisenstein)

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

Kronecker Theorem;

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

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 $\forall i = 1, \dots, n$

$< p_1(x) >$ is maximal.

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

Put $E = \frac{F[x]}{<p_1(x)>}$

Define $\emptyset = F \rightarrow \frac{F[x]}{<p_1(x)>} \quad by \ \ \emptyset(a) = a+< p_1(x) > \ \ \forall a \in F$

(1) $\emptyset$ is well define :

$$if \ \ a = b \ \rightarrow \ a+< p_1(x) > = b+< p_1(x) > \ \rightarrow \ \emptyset(a) = \emptyset(b)$$

(2) $\emptyset$ is well homomorphism?

$$\emptyset(a+b) = a+b+< p_1(x) > = a+< p_1(x) > + b+< p_1(x) > = \emptyset(a) + \emptyset(b)$$

$$\emptyset(a.b) = a.b + < p_1(x) > = (a + < p_1(x) >) \cdot (b + < p_1(x) >)$$
$$= \emptyset(a) \cdot \emptyset(b)$$

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

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

$a + < p_1(x) > = b + < p_1(x) > \leftrightarrow a - b \in < p_1(x) >$,

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

$F \subset E = \frac{F[x]}{<p_1(x)>}$, $\therefore E$ is extension for F

Let $\propto \in E$, $\propto = x + < p_1(x) >$, $x \in F[X]$

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

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

$if \ \ p_1(\propto) = 0 \rightarrow f(\propto) = 0$

If $deg\, p_1(\propto) \geq 1$, $p_1(x) = a_0 + a_1 x + \cdots + a_n x^n$

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

$p_1 (x + < p_1(x) >) = a_0 + a_1 x + a_2 x^2 \ldots + a_n x^n + < p_1(x) >$

$= p_1(x) + < p_1(x) >$

$= < p_1(x) > = 0$

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

H.W/

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

Sol/ Define $h: C \rightarrow \frac{R[x]}{<x^2+1>}$ by $h(a + ib) = a + bx + < x^2 + 1 >$

1) $h(a+ib) = h(c+id)$

$a + bx + < x^2 + 1 > = c + dx + < x^2 + 1 >$

$\rightarrow a + bx - c - dx \in < x^2 + 1 >$

$\rightarrow a + bx - c - dx = 0 \rightarrow a - c = 0 \ , \ b - d = 0$

$\rightarrow a = c \quad \& \quad b = d \rightarrow a + ib = c + id \ , \ \therefore 1-1$

2) h is homomorphism

$h(a + ib + c + id) = h(a + c + (b+d)i)$

$= a + c + (b+d)x + < x^2 + 1 > = a + bx + < x^2 + 1 > \ c + dx + c$

$= h(a+ib) + h(c+id)$.

$h(a+ib).(c+id) = h(a+ib).h(c+id))$

Example:;

$f(x) = x^4 - 4 \in Q[x]$

$f(x) = (x^2 - 2)(x^2 + 2)$

Use Kronecker's Thmeorem , $\propto = x + < p_1(x) > = x + < (x^2 - 2) >$

H.W//

1)let $f(x) = x^2 + 5$ prove that $< f(x) >$ is irreducible in $Z[x]$ ($Hint$: $\emptyset : z[x] \rightarrow Z[\sqrt{-5}]$, $\emptyset(\mathrm{g}(\mathrm{x})) = \mathrm{g}(\sqrt{-5})$)

2) $f(x) = x^4 + x^2 = 1 \in Q[x]$,is f irreducible and have a root in Q?

3) $f(x) = x^3 + \overline{3}$ 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)$f(x)$ $is\ irr$educible iff $f(x+1)$ is irreducible in Q .

2) $f(x)$ is irreducible , iff $f(x-1)$ is irreducible in Q .

3)The polynomial $f(x) = 1 + x + x^2 + \cdots + x^{p-1}$ (where P is prime) is irreducible in $Q[x]$?

Proof:

(1) & (2) $(H.W)$

Proof: (3)

$$f(x+1) = 1 + (x+1) + (x+1)^2 + \cdots + (x+1)^{p-1}$$

$$= \frac{(x+1)^p - 1}{(x+1)-1} = \frac{(x+1)^p - 1}{x}$$

$$= \frac{1}{x}[(x+1)^p - 1]$$

$$= \frac{1}{x}\left[x^p + px^{p-1} + \frac{p(p-1)}{2!}x^{p-2} + \cdots + px\right]$$

$$= \left[x^{p-1} = px^{p-2} + \frac{p(p-1)}{2!}x^{p-3} + \cdots + p\right].$$

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: $E = \frac{Q[x]}{<x^2-2>}, \propto = x + < x^2 - 2 >$

H.W//

Let $f(x) = x^2 + 5x + 8$, is $f(x)$ irreducible on Q ?

Hint: $f(x+1) = \cdots$

Defintion:

Let E be an extension field of F, let $\propto \in E$ we called $\propto$ algebraic element if there exists a non zero polynomial $f(x) \in F[x]$ $s.t$ $f(\propto) = 0$.

Otherwise we say that $\propto$ 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) $\propto = \sqrt{1+\sqrt{3}} \in R$ algebraic on Q ?

2) π is algebraic on Q ?

3) e is algebraic on Q ?

Sol: (1) $\propto^2 = 1+\sqrt{3} \rightarrow \propto^2 - 1 = \sqrt{3} \rightarrow (\propto^2 - 1)^2 = 3$

$\propto^4 - 2\propto^2 - 1 = 3 \rightarrow \propto^2 - 2\propto^2 - 4 = 0$.

Defintion::

Let R is I.D $f(x) \in R[x]$ non-constant, f is irreducible iff $\nexists\ h(x)\ ,\ k(x) \in R[x]\ \ s.t\ \ f(x) = h(x).k(x)\ ,\ deg\big(h(x)\big) \geq 1, \deg\big(k(x)\big) \geq 1$

Example:

$f(x) = 2x^2 - 4 \in Z[x]$,

$f(x) = 2(x^2-2) = 2\big(x-\sqrt{2}\big)\big(x+\sqrt{2}\big)$

$\sqrt{2} \notin Z$

Note: $f(x) = ax + b \in R[x]$ is irreducible

$f(x) = h(x).k(x)$ since $\deg f(x) < \deg(h(x)\cdot k(x))$

Example:

$f(x) = x^3 + 3x + 2 \in Z_5[x]$?

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.

$i.e)$ $h(x) = x - a$, $a \in Z_5[x]$ $h(a) = a - a = 0$ and since $f(x) = h(x)\cdot k(x) = (x-a)\cdot k(x)$, $\therefore f(a) = (a-a)\cdot k(a) = 0$

$\therefore f$ has a root in $Z_5[x]$ but f has no root in $Z_5[x]$ since

$f(a) = 2$, $f(1) = 1$, $f(2) = 1$, $f(3) = 3$, $f(4) = 78$ $C!$ With $f(x) = h(x) \cdot k(x)$ $\therefore f$ 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:

$f(x) = 2x^2 + 4 \in R[x]$

$= 2(x^2 + 2) = 2\left(x - \sqrt{2}i\right)\left(x + \sqrt{2}i\right)$ $\therefore f$ has no root in R $\therefore f$ is irreducible

Example:

$f(x) = x^3 + 3 \in Z_6[x].$

$f(0) = 3$, $f(1) = 4$, $f(2) = 5$, $f(3) = 0$

$\therefore f$ *is not irreducible*

Example(H.W)

$f(x) = x^3 + x + 1 \in Z_5[x]$.

Example(H.W)

$f(x) = x^2 + 3 \in Z_7[x].$