UNIT-V

3.6 - The field of quotients of an Integral Domain
3.7 - Euclidean Rings

Defn (R என்பது R'க்கு இயல்பொருமையான உட்கொள்ளத்தக்கது இருக்குமேயானால் R' ஆனது R-ஐ உள்ளடக்கிய (imbedded) எனப்படும்)

A Ring R can be imbedded in a ring R' if there is an isomorphism of R into R'.

R' will be called over-ring (or) extension of R, if R can be imbedded in R'.

field
$R[x_1, x_2, \dots x_n] \to$ I.D

Thm: 3.6.1 Every Integral domain can be imbedded in a field.
(ஒவ்வொரு எண் அரங்கத்தையும் ஒரு களம் தன்னகத்தே கொண்டு இருக்கும்)

lemma 3.2.2

Pf:

Suppose that D is an integral domain.

Let $R = \{(a,b) / a, b \in D, b \neq 0\}$. Take $(a,b) = \frac{a}{b}$.

Define a relation $\sim$ on R by,

$(a,b) \sim (c,d)$ iff $ad = bc$

$\boxed{\frac{a}{b} = \frac{c}{d} = ad = bc}$

we now show that $\sim$ is an equivalence relation.
(சமானத் தொடர்பு)

(i) since $ab = ba$

$\therefore (a,b) \sim (a,b)$

$\therefore \sim$ is reflexive. (தன் மாற்றுத் தன்மை)

(ii) $(a,b) \sim (c,d) \quad \therefore ad = bc$

$(c,d) \sim (a,b) \quad \because cb = ad.$

$\therefore \sim$ is symmetric (சமச்சீர் பண்பு)

(iii) $(a,b) \sim (c,d) \quad \therefore ad = bc$ — ①

$(c,d) \sim (e,f) \quad \therefore cf = de$ — ②

① × f gives,

$adf = bcf$

② × b gives, $bcf = bde$

$\therefore adf = bde$

$(af - be)d = 0$

Since D is an integral domain. so it has no zero divisors.

$\therefore d \neq 0$ gives $af - be = 0$ ie) $af = be$ $\left[\frac{a}{b} = \frac{e}{f}\right]$

$(a,b) \sim (e,f)$

$\therefore \sim$ is transitive. (கடந்தற் தன்மை)

$\therefore \sim$ is an equivalence relation on R.

Denoting the equivalence class of (a,b) by $[a,b]$

Set, $F = \{[a,b] / a,b \in D, b \neq 0\}$ $[\underbrace{x_1, x_2}_{(x_1,x_2)}, x_3, \ldots x_n]$

we prove the following,

(i) F is a field under suitable operations.
(இரும்பட செயலைப் பொருத்து F ஒரு களம் என நிரூபிக்கோம்)

(ii) D is imbedded into F.
(D ஐ F இனுள் தன்னகத்தே கொண்டிருக்கும் என நிரூபிக்கோம்)

First define $+$ on F by,

closure property $[a,b] + [c,d] = [ad + bc, bd] \neq 0$. $\left[\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}\right]$

$+$ As $b \neq 0, d \neq 0$ & D is an integral domain, it follows $bd \neq 0$.

$\therefore [ad + bc, bd] \in F$.

$\therefore$ closed.

We now prove that addition is well defined.

closure property suppose $[a,b] = [a',b']$

$[c,d] = [c',d']$

$\therefore ab' = ba'$ and $cd' = dc'$

we have to show ~~$[a'd' + b'c', b'd']$~~ =

$[\underset{ad}{ab} + bc, bd] = [a'd' + b'c', b'd']$

Consider,

$(ad+bc)\,b'd' = ad\,b'd' + bc\,b'd'$

$= ab'dd' + bb'cd'$

$= ba'dd' + bb'dc'$

$= bd(a'd' + b'c')$

$\therefore [ad+bc, bd] = [a'd' + b'c', b'd']$

(ii) $[a,b] + [c,d] = [a'b'] + [c', d']$

$\therefore$ '+' is well defined on F.

Consider, Associative

$([a,b] + [c,d]) + [e,f] = [ad+bc, bd] + [e,f]$

$= [adf + bcf + bde, bdf]$

$[a,b] + ([c,d] + [e,f]) = [a,b] + [cf + de, df]$

$= [adf + bcf + bde, bdf]$

$\therefore$ RHS of both are equal

$\therefore$ Associative.

identity property $[0,1]$ acts as the zero element of F with $1 \in D$.

If $d \neq 0$ then $[0,1] = [0,d]$

$\therefore [0,d]$ is the zero element of F.

Inverse property $[+a,b] + [-a,b] = [0, b^2]$ where $b^2 \neq 0$

$\therefore [-a,b]$ is the additive inverse of $[a,b]$

Since D is a commutative ring, F is an abelian group under addition.

Now define multiplication operation on F by

$[a,b]\,[c,d] = [ac, bd]$

To prove it is well defined one,

$[a,b] = [a',b']$ $\quad \therefore ab' = a'b$

$[e,d] = [c',d']$ $\quad \therefore cd' = dc'$

∴ To prove $[ac, bd] = [a'c', b'd']$

So consider,

$$ac\,b'd' = ab'cd'$$
$$= a'bdc'$$
$$= bd\,a'c'$$

$\therefore [ac, bd] = [a'c', b'd']$

Closure

&) $[a,b]\,[c,d] = [a',b']\,[c',d']$

$\therefore$ well defined.

As $b \neq 0$, $d \neq 0$ and D is integral domain, $bd \neq 0$.

$\therefore [ac, bd] \in F$.

$\therefore$ closed.

Identity $[1,1]$ is the unit element of F with $1 \in D$.

$$[1,1] = [d,d]$$

$[d,d]$ is the unity of F.

Consider,

Distributive
$$[a,b]([c,d] + [e,f]) = [a,b]\,[cf + de, df]$$
$$= [acf + ade, bdf]$$
$$[a,b]\,[c,d] + [a,b]\,[e,f] = [ac, bd] + [ae, bf]$$
$$= [acbf + bdae, b^2df]$$
$$= [acf + ade, bdf]\,[b,b]$$
$$= [acf + ade, bdf]$$

$\therefore$ RHS of both are equal.

$\therefore$ Distributive.

Commutative Since D is commutative, F is commutative.

If $[a,b] \neq 0 \in F$ then $a \neq 0$ and $b \neq 0$.

Inverse Consider, $[a,b]\,[b,a] = [ab, ab]$
$$= [1,1]$$

$\therefore [b,a]$ is the inverse of $[a,b]$

Thus F is a field.

To prove (ii)

1-1

Define $\varphi : D \to F$ by

$$\varphi(a) = [a,1] \quad \forall\, a \in D$$

To prove it is 1-1.

Take, $[a,1] = [b,1]$

$$a = b.$$

$\therefore \varphi$ is 1-1.

Consider,

$$\varphi(a+b) = [a+b, 1]$$

onto

$$= [a,1] + [b,1]$$

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

Also $\varphi(ab) = [ab, 1]$

$$= [a,1]\,[b,1]$$

homomo

$$= \varphi(a)\varphi(b)$$

$\therefore \varphi$ is a homomorphism.

Further $\varphi(1) = [1,1]$

Take $D' = \{[a,1] / a \in D\}$

$\therefore D' \subset F$ & $D \cong D'$.

Thus D is imbedded into F.

Note: F is called the field of quotients of D.

UNIT-V (2016-2018)

3.7: Euclidean Ring

(Unique factorization)

(X) **Defn**

An integral domain R is said to be a Euclidean ring if for every $a \neq 0$ in R there is non negative integer $d(a)$ such that

(1) for all $a, b \in R$, both non-zero, $d(a) \leq d(ab)$

(2) For any $a, b \in R$, both non zero, there exists $t, r \in R$ such that $a = tb + r$ where either $r = 0$ (or) $d(r) < d(b)$.

(X) **Thm 3.7.1:** Let R be a Euclidean ring and let A be an ideal of R. Then there exist an element $a_0 \in A$ such that A consists exactly of all $a_0 x$ as x ranges over R.

(or)

✓ Every Euclidean ring is a principle ideal domain (PID) (or) principle ideal ring.

Pf: Let R be an Euclidean ring.

$\because R$ is an integral domain, it is enough to prove that every ideal of R is a principal ideal.

Let A be an ideal of R.

we claim that, A is a principal ideal.

If $A = 0$, take $a_0 = 0$, $\therefore$ Theorem holds.

So assume that $A \neq (0)$, then there exist an element $a \neq 0$ in A.

Take $a_0 \in A$ such that $d(a_0)$ is minimal among all $d(a)$ in R.

i.e) $d(a_0)$ is less than $d(a)$

i.e) $d(a_0) < d(a)$.

now, we'll prove that $A = (a_0)$ → multiple of a_0 i.e $a = tb + r$

Since R is an Euclidean ring for $a, a_0 \in A$ i.e) a, a_0 in R.

(By 2nd property)

By 2nd property of Euclidean ring $a = tb + r$

there exist $t, r \in R$ such that $a = ta_0 + r$. where $r = 0$ (or)

$$d(r) < d(a_0).$$

Since A is an ideal of R,

$a_0 \in A$, $t \in R$, $ta_0 \in A$. (by By (2) $ta_0 \in A$ $a = tb$ (i.e) $a = tb + r$)

(i.e) $a \in A$, $ta_0 \in A$ gives $a - ta_0 \in A$. ($a, a_0 \in A$)

(ii) $r = (a - ta_0) \in R$. $\Rightarrow r = a - tb$

$r = a - ta_0$

(iii) $r \in R$. $a = ta_0 + r$

If $r \neq 0$, $d(r) < d(a_0)$ gives the contradiction to $d(a_0)$ is minimal.

$\therefore r = 0$, $\therefore a = ta_0$ $\forall$ $t \in R$ & $a \in A$.

Since a is arbitrary. Every element of A is expressed as a multiple of a_0. (i.e) $a = ta_0$.

$\therefore a_0$ is generator of A.

$\therefore$ A is a principal ideal generated by a_0.

$A = \{xa_0 / x \in R\}$ (multiple of a_0)

Since A is arbitrary every ideal of R is principal ideal.

Thus, R is a principal ideal domain. (2)

& t ranges over R.

$\therefore$ Every Euclidean ring is a principal ideal domain (PID)

Hence the proof.

Note The notation $(a) = \{xa / x \in R\}$ to represent the ideal of all multiples of a.

Defn: principal ideal ring / domain (X)

An integral domain R with unit element is a principal ideal ring if every ideal A in R is of the form $A = (a)$ $\forall$ $a \in R$.

(eg) The ring of integers $(I, +)$ is a principal ideal ring (PIR)

Thm: A Euclidean ring possess a unit element. (ஒற்றை உறுப்பு)

Pf: Let R be an element.

i) Rf is an ideal of $R \cdot R = (u_0)$ $\forall u_0 \in R$.

All the elements of R are the multiples of u_0.

$u_0 \in R \Rightarrow u_0 = u_0 \cdot c$, $c \in R$.

let $a \in R \Rightarrow a = x \cdot u_0$, $x \in R$.

Consider, $ac = (xu_0) \cdot c = x(u_0 c) = xu_0 = a$.

$\therefore ac = a$ $\forall$ $a \in R$.

$\Rightarrow c$ is the unit element.

$A \in R$ posses a unit element.

Defn Divide of R

① If $a \neq 0$ and b are in a commutative ring R then a is said to divide b if there exist $c \in R$ such that $b = ac$.

we use the symbol a/b

Greatest common Divisor (GCD) (மீப்பெரு பொது காரணி)

② If $a, b \in R$ then $d \in R$ is said to be a greatest common divisor of a and b if

i) d/a and d/b

2) whenever c/a and c/b then c/d.

we denote $d = (a, b)$

Lemma 3.7.1

(L) Let R be a Euclidean ring. Then any two elements a and b in R have a greatest common divisor d. Moreover $d = \lambda a + \mu b$ for some $\lambda, \mu \in R$.

Pf: let $A = \{ra + sb / r, s \in R\}$

To prove A is an ideal of R.

5) closure law

let $x, y \in A$.

$\therefore x = r_1 a + s_1 b$

$y = r_2 a + s_2 b$.

$x + y = (r_1 + r_2) a + (s_1 + s_2) b$

$r_1 + r_2 \in R$, $s_1 + s_2 \in R$.

$\therefore x + y \in A$.

$\therefore$ closed.

6) Inverse law

let $x \in A$

$\Rightarrow x = ra + sb$

$-x = -ra - sb$

$= (-r) a + (-s) b \in A$, $-r_1, -s_1 \in R$.

$\therefore A$ is a subgroup under '+'.

$\Rightarrow -x \in A$.

$\therefore$ Inverse exists. $(x + (-x) = 0$

For any $u \in R$,

consider $ux = u(r_1 a + s_1 b)$

$= (ur_1) a + (us_1) b \in A$ $ur_1, us_1 \in R$.

$\therefore A$ is an ideal of R.

Since A is an ideal of R, (By Thm 3.7.1) ie) there exist an element $d \in R$ such that every element of A is the multiples of d. ie $A = \{xd / x \in R\}$ ——— (1)

$\therefore d \in A$ is of the form $ra + sb$.

$\therefore d = \lambda a + \mu b$ for some $\lambda, \mu \in R$. ——— (2)

(By Cor : 3.7.1),

Euclidean ring R has a unit element 1.

$\therefore 1 \in R$.

$a = 1 \cdot a + 0 \cdot b \in A$

$b = 0 \cdot a + 1 \cdot b \in A$ $\because 1, 0 \in R$.

$\therefore a, b \in A$.

by (2), a & b are multiples of d.

$\therefore d/a$ and d/b.

This proves condition ① of gcd.

Let c/a and c/b

Then $c/\lambda a$ and $c/\mu b$

$\therefore c/\lambda a+\mu b \Rightarrow c/d$ by (2).

This proves (2) condition of gcd.

$\therefore d$ is the gcd of a & b where $d=\lambda a+\mu b$.

Defn Let R be a commutative ring with unit element. An element $a \in R$ is a unit (அலகு) in R if there exists an element $b \in R$ such that $ab=1$.

Note Unit in a ring is an element whose inverse is also in the ring.

(eg) Ring of integers.

$1 \cdot 1 = 1$, $-1 \cdot -1 = 1$. (inverse exists).

Lemma 3.7.2 (ஒன்றுக்கொன்று ஏறும் அலகு) Let R be an integral domain with unit element and suppose that for $a, b \in R$ both a/b and b/a are true. Then $a=yb$, where y is a unit in R.

Pf: Since a/b,

$\therefore b=xa$ for some $x \in R$.

Since b/a, $a=yb$ for some $y \in R$.

Thus $b=xa$

$=xyb$

$=(xy)b$

Since D is an integral domain. $b(xy-1)=0$ & $b \neq 0$

$\Rightarrow xy=1$.

Thus y is the unit in R.

$\therefore a=yb$ where y is the unit.

$u - v = e^{-}(\cos y - \sin y)$

Q:12

① Section: 16

① Theory - 2

② C-Requat

|

Necessary conditions

③ Sufficient polar

④ polar conditions

⑤ Analytical (Harmonic function - Theory)

⑥ → Problem — ② → Question

⑦ ③ Q

⑧ ⑦ Q

⑨ ⑨ - Q

⑩ 12 → Q

Total 10 submission

Tuesday (4:00 pm)

Defn let R be a commutative ring with unit element. Two elements a and b in R are said to be <u>associates</u> if $b = ua$ for some unit u in R.

Lemma 3.7.3

(X) let R be a Euclidian ring and $a, b \in R$. If $b \neq 0$ is not a unit in R, then $d(a) < d(ab)$.

Pf Given R is an Euclidean ring.

let $A = (a)$ be an ideal of R generated by 'a'. then $d(a)$ is a minimum value in R. (ie every element of A is the multiples of a)

ie) $A = (a) = \{xa / x \in R\}$.

<u>Now prove A is the ideal.</u>

let $u_1, u_2 \in A$

$\therefore u_1 = x_1 a$

$u_2 = x_2 a$

Consider, $u_1 + u_2 = (x_1 + x_2)a$ where $(x_1 + x_2) \in R$

$\therefore (x_1 + x_2) a \in A$.

$\therefore u_1 + u_2 \in A$ $\therefore$ closed.

Consider, $-u = -x_1 a \in A$ Since $-x_1 \in R$.

$\therefore -u_1$ is the inverse of u_1.

$\therefore$ Inverse exists.

$\therefore A$ is the subgp under addition.

<u>Take $u_1 \in A$ & $r \in R$</u>

consider $u_1 r = (x_1 a) r$

$= x_1 (ar) = x_1 (ra)$

$= (x_1 r) a$

$\therefore$ commutative.

Since $x_1, r \in R$ $\therefore (x_1 r) a \in A$.

$\therefore u_1 r \in A$.

$\therefore A$ is the ideal.

By condition (1) of a Euclidean ring,

$d(a) \leq d(xa)$ for $x \neq 0$ in R.

This $d(a)$ is the minimum in A

Now $ab \in A$ (ideal) $\forall\ a \in A, b \in R$.

$\therefore d(a) \leq d(ab)$.

Suppose that $d(a) = d(ab)$

Since $d(a)$ is minimal & $d(ab)$ is minimal in A,

$\therefore$ every element in A is a multiple of ab. → By Thm 3.7.1 $d(a)$ is min. We have proved every elt in A is a multiple of a.

In particular, $a \in A$

$\therefore a$ must be multiple of ab.

$\therefore a = abx$ for some $x \in R$.

Since $a \neq 0$, $bx = 1$.

$\therefore b$ is a unit in R.

$\Rightarrow \Leftarrow$

$\therefore d(a) < d(ab)$.

Defn In the Euclidean Ring R, a nonunit π is said to be a *prime element* of R if whenever $\pi = ab$, where a, b are in R, then one of a (or) b is a unit in R.

Lemma 3.7.4 Let R be a Euclidean ring. Then every element in R is either a unit in R or can be written as the product of a finite number of prime elements of R.

Pf Let $a \in R$.

We prove this by induction on $d(a)$.

If $d(1) = d(1)$ — (1).

we now prove a is unit in R.

suppose a is not a unit in R.

by lemma 3.7.3, $d(1) < d(1.a)$

$d(1) < d(a)$ ⇒⇐ to (1),

$\therefore$ a is a unit.

which proves the lemma.

we assume that the lemma is true for all $x \in R$ such that $d(x) < d(a)$.

we now prove the lemma is true for 'a' also.

If a is the prime element there is nothing to prove.

Suppose that, $a = bc$, where neither b nor c is a unit
(i.e) b & c not a unit)

by lemma 3.7.3

$d(b) < d(bc) = d(a)$

Illly $d(c) < d(bc) = d(a)$

since $d(b) < d(a)$ $\because a = bc$

By ~~hyp~~ induction hypothesis,

$b = \pi_1 \cdot \pi_2 \cdots \pi_n$ —— (1) where π's are prime elements in R.

since $d(c) < d(a)$

By induction hypothesis,

$c = \pi_1' \cdot \pi_2' \cdots \pi_n'$ —— (2)

where π''s are prime elements in R.

$\therefore a = bc$

$= \pi_1 \pi_2 \ldots \pi_n \pi_1' \ldots \pi_n'$

= product of finite number of prime elements.

$\therefore$ thm is true for a.

Defn: In the Euclidean ring R, a and b in R are said to be relatively prime if their greatest common divisor is a unit of R.

Lemma 3.7.5

(X) Let R be a Euclidean ring. Suppose that for $a, b, c \in R$, a/bc but $(a,b)=1$. Then a/c.

Pf Given a & b are relatively prime in R.

$\therefore$ GCD of $(a,b)=1$.

$\therefore \lambda a + \mu b = 1$ ($\because$ by lemma 3.7.1) —①

mul: ① by 'c', gives

$\lambda ac + \mu bc = c$ —②

Given that $a/bc = a/\mu bc$

It is clear that $a/ac = a/\lambda ac$

$\therefore a/\lambda ac + \mu bc$

$\Rightarrow a/c(\lambda a + \mu b)$

$\Rightarrow a/c$. (by ②)

Lemma 3.7.6

If π is a prime element in the Euclidean ring R and π/ab where $a, b \in R$ then π divides atleast one of a (or) b. [ie) π/a (or) π/b.]

Pf

π in R is a prime element.

let $a \in R$

If $(\pi/a) = \pi$ then π/a.

If $(\pi \not/ a)$ then $(\pi/a) = 1$.

By Lemma 3.7.5,

$\pi / ab \Rightarrow \pi / b$

$\therefore \pi / ab \Rightarrow \pi / a$ (or) π / b.

Corr If π is a prime element in the Euclidean ring R and $\pi / a_1 a_2 \ldots a_n$ then π divides at least one $a_1, a_2, \ldots, a_n$.

Pf $\pi / a_1 (a_2, a_3 \ldots, a_n)$

By Lemma, π / a_1 (or) $\pi / a_2, \ldots a_n$

$\pi / a_2, \ldots a_n \Rightarrow \pi / a_2$ (or) $\pi / a_3, \ldots, a_n$.

proceeding in this manner,

π / a_1 (or) $\pi / a_2 \ldots \pi / a_n$.

Thm 3.7.2 [Unique Factorization Theorem]

Let R be a Euclidean ring and $a \neq 0$ a nonunit in R. Suppose that $a = \pi_1, \pi_2 \cdots \pi_n = \pi_1' \pi_2' \ldots \pi_m'$ where the π_i and π_j' are prime elements of R. Then $n = m$ and each π_i, $1 \leq i \leq n$ is an associate of some π_j', $1 \leq j \leq m$ and conversely each π_k' is an associate of some π_q.

Pf let $a = \pi_1 \pi_2 \ldots \pi_n = \pi_1' \pi_2' \ldots \pi_m'$ where π_i & π_j' are prime elements in R.

To prove, $n = m$ and each π_i is an associate of some π_j'.

Now, $\pi_1 / \pi_1, \pi_2, \ldots \pi_n$

and hence $\pi' / \pi_1', \pi_2' \ldots \pi_m'$.

Since π_1 is prime, π_1' must divide some π_k'.

Thus, $\frac{\pi_1}{\pi_1'}$ and therefore $\pi_1' = u_1 \pi_1$ for some element $u_1 \in R$
(by associate defn)

Since π_1' is a prime element
we find that u_1 is a unit in R.

$\therefore \pi_1$ and π_1' are associates.

Thus $\pi_1 \pi_2 \dots \pi_n = \pi_1' \pi_2' \dots \pi_m'$
$= u_1 \pi_1 \pi_2' \dots \pi_m'$

$\Rightarrow \pi_2 \pi_3 \dots \pi_n = u_1 \pi_2' \pi_3' \dots \pi_m'$

proceeding this, on this relation with π_2.

After n steps, the LHS becomes,

the RHS is a product of a certain number of π'.

[ie $1 = u_1 u_2 \dots u_n$ (a pdt of $(m-n)\pi'$s) where $u_1, u_2 \dots$ are units]

$\therefore n \le m$. — ①

since the π' are not units
so $\Rightarrow\Leftarrow$ to ①, → (As no prime elt is a unit)

III^{ly} $m \le n$. — ②

$\therefore$ from ① & ②, $n = m$.

every π_i has some π_i' as an associate. & conversely.

lemma 3.7.7

The ideal $A = (a_0)$ is a maximal ideal of the Euclidean ring R. iff a_0 is a prime element of R.

Pf. suppose that $A = (a_0)$ is the maximal ideal to prove a_0 is the prime element.

Take a_0 is not the prime element & we bring one contradiction.

Since a_0 is not the prime element.

$a_0 = bc$ where $b, c \in R$.

and neither b nor c is a unit — ①
(இங்கு b-யோ c-யோ அலகாக இருக்க வேண்டும்)

let $B = (b)$.

$\therefore A \subset B \subset R$.

since A is the maximal ideal
(ಗರಿಷ್ಠ ಐಡಿಯಲ್)

Take $B = R$

$1 \in R$

$\therefore 1 \in B$.

$\therefore 1 = xb$ for some $x \in R$.

This $\Rightarrow$ b is a unit in R.

which is $\Rightarrow \Leftarrow$ to (1)

Ily Take $A = B$.

$\therefore b \in B = A$

$\therefore b = xa_0$ for some $x \in R$.

put $a_0 = bc$

$= xa_0c$

$= xca_0$

Since R is an integral domain.

$xc = 1$.

This $\Rightarrow$ c is a unit in R.

which is a $\Rightarrow \Leftarrow$ to (1).

$\therefore$ This contradiction arises by taking a_0 is not the prime.

$\therefore a_0$ is the prime element of R.

Conversely,
(ವ್ಯತಿರಿಕ್ತವಾಗಿ)

Suppose that a_0 is the prime element of R.

Let U be an ideal of R such that (U ಇರುವಂತೆ R-ನ ಗರಿಷ್ಠ ಐಡಿಯಲ್)

$A = (a_0) \subset U \subset R$.

let $U = (u_0)$ for some $u_0 \in R$.

Since $A \subset U$

$a_0 \in (u_0) \Rightarrow a_0 = xu_0$ for some $x \in R$.
(ಏಕೆಂದರೆ)

Since a_0 is a prime element either x or u_0 is a unit in R.

If u_0 is a unit in R then $U = R$.

If x is a unit in R, $x^{-1} \in R$.

$$\text{Let, } a_0 = x u_0$$

$$\Rightarrow x^{-1} a_0 = u_0.$$

$$\therefore u_0 = x^{-1} a_0$$

$x^{-1} \in R$, $a_0 \in A \Rightarrow x^{-1} a_0 \in A$.

$$\therefore u_0 \in A$$

$$\therefore U \subset A$$

$$\therefore U = A$$

$\therefore$ there is no ideal of R inbetween A & R.

$\therefore$ A is the maximal ideal of R.

UNIT-V

POLYNOMIAL RINGS.

3.9. **Def:**

If $P(x) = a_0 + a_1 x^1 + \cdots + a_m x^m$,

$q(x) = b_0 + b_1 x^1 + \cdots + b_n x^n$ are in $F[x]$.

$a_0, a_1, \ldots, a_m, b_0, b_1, \ldots, b_n \in F$ then $P(x) = q(x)$ iff for every Integer $i \geq 1$ greater than are equal to zero $a_i = b_i$. [i.e., 2 polynomials declared to be equal iff, their corresponding co-efficient are equal].

2. If $P(x) = a_0 + a_1 x^1 + \cdots + a_m x^m$ and $q(x) = b_0 + b_1 x^1 + \cdots + b_n x^n$ are both in $F[x]$, then $P(x) + q(x) = c_0 + c_1 x^1 + \cdots + c_t x^t$ where for each i, $c_i = a_i + b_i$.

Ex:-

Let $P(x) = 1 + x$ and $q(x) = 3 - 2x + x^2$.

$a_0 = 1$, $a_1 = 1$, $b_0 = 3$, $b_1 = -2$, $b_2 = 1$ then

$P(x) + q(x) = c_0 + c_1 x^1 + c_2 x^2 + \cdots$

$c_0 = a_0 + b_0$

$= 1 + 3 = 4$.

$c_1 = a_1 + b_1$

$= 1 - 2 = -1$

$c_3 = a_3 + b_3$

$= 0$.

$\therefore P(x) + q(x) = 4 - x + x^2$.

3. **Def:**

If $p(x) = a_0 + a_1 x + \cdots + a_m x^m$ and

$q(x) = b_0 + b_1 x + \cdots + b_n x^n$

then $p(x) \cdot q(x) = c_0 + c_1 x + \cdots + c_k x^k$.

where $c_t = a_t b_0 + a_{t-1} b_1 + \cdots + a_0 b_t$.

Ex:

Let $p(x) = 1 + x - x^2$, $q(x) = 2 + x^2 + x^3$.

$a_0 = 1$ $a_1 = 1$ $a_2 = -1$ $a_3 = a_4 = a_5 = \cdots = 0$.

$b_0 = 2$ $b_1 = 0$ $b_2 = 1$ $b_3 = 1$ $b_4 = b_5 = \cdots = 0$.

then $p(x) \cdot q(x)$

$c_0 = a_0 b_0 = 1(2) = 2$.

$c_1 = a_1 b_0 + a_0 b_1 \Rightarrow c_1 = (1)(2) + (1)(0) = 2$.

$c_2 = a_2 b_0 + a_1 b_1 + a_0 b_2 \Rightarrow c_2 = (-1)(2) + (1)(0) + (1)(1)$

$= -2 + 0 + 1 = -1$.

$c_3 = a_3 b_0 + a_2 b_1 + a_1 b_2 + a_0 b_3$.

$= 0 + (-1)(0) + (1)(1) + (1)(1) = 2$.

$c_4 = a_4 b_0 + a_3 b_1 + a_2 b_2 + a_1 b_3 + a_0 b_4$

$= 0 + 0 + (-1)(1) + (1)(1) + (1)(0)$

$= -1 + 1 = 0$.

$c_5 = a_5 b_0 + a_4 b_1 + a_3 b_2 + a_2 b_3 + a_1 b_4 + a_0 b_5$

$= 0 + 0 + 0 + (-1)(1) + 0 + 0$

$= -1$.

$c_6 = a_6 b_0 + a_5 b_1 + a_4 b_2 + a_3 b_3 + a_2 b_4 + a_1 b_5 + a_0 b_6$

$= 0 + 0 + 0 + 0 + (-1)(0) + (1)(0) + 0$

$= 0$.

$\therefore c_6 = c_7 = c_8 = \cdots = 0.$

$\therefore p(x)q(x) = c_0 + c_1 x + \cdots$

$= 2 + 2x - x^2 + 2x^3 + 1x^4 - x^5$

$= 2 + 2x - x^2 + 2x^3 - x^5.$

1). P.T $F[x]$ is a ring w.r.t addition & Multiplication.

(i) Let $p(x), q(x) \in F[x]$,

$p(x) = a_0 + a_1 x^1 + \cdots + a_m x^m.$

$q(x) = b_0 + b_1 x^1 + \cdots + b_n x^n.$

$p(x) + q(x) = c_0 + c_1 x + \cdots + c_t x^t \in F[x]$,

$c_i = a_i + b_i$, for each i.

$\therefore p(x) + q(x) \in F[x].$

$\therefore$ closed.

(ii) By the definition Associative property is true.

(iii) Let $p(x) \in F[x]$, there exist

$i(x) = 0 + 0x + 0x^2 + \cdots + 0x^n \in F[x].$

such that,

$p(x) + i(x) = (a_0 + a_1 x^1 + \cdots + a_m x^m) +$
$(0 + 0x + 0x^2 + \cdots + 0x^n)$

$= a_0 + a_1 x^1 + \cdots + a_m x^m.$

$= p(x).$

(i.e.,) $p(x) + i(x) = p(x).$

$\therefore 0 + 0x + 0x^2 + \cdots + 0x^n$ is the Identity element

(or) zero element of $F[x]$.

(iv) Let $p(x) \in F[x]$, $\exists\ -p(x) \in F[x]$

such that,

$$p(x) + (-p(x)) = a_0 + a_1 x^1 + \cdots + a_m x^m +$$
$$(-a_0 + (-a_1)x^1 + \cdots + (-a_m)x^m)$$
$$= a_0 - a_0 + (a_1 - a_1)x^1 + \cdots + (a_m - a_m)x^m$$
$$= 0 + 0\cdot x + \cdots + 0x^m$$
$$= i(x).$$

$\therefore$ $-p(x)$ is the Inverse element of $p(x)$.

(V) Let $p(x), q(x) \in F[x]$.

Now

$$p(x) + q(x) = c_0 + c_1 x + \cdots + c_t x^t,$$

for each i, $c_i = a_i + b_i$, $a_i, b_i, c_i \in F$

$$q(x) + p(x) = d_0 + d_1 x + \cdots + d_t x^t,$$

for each i, $d_i = b_i + a_i$,

since,

F is a Field, $a_i + b_i = b_i + a_i$ for each i

$\therefore$ $c_i = d_i$ for each i.

$\therefore$ $p(x) + q(x) = q(x) + p(x)$.

$\therefore$ commutative law is true.

(vi) Let $p(x), q(x) \in F[x]$.

Now $p(x)\,q(x) = c_0 + c_1 x + \cdots + c_k x^k \in F[x]$.

where $c_t = a_t b_0 + a_{t-1} b_1 + \cdots + a_0 b_t$.

$\therefore$ $p(x)\,q(x) \in F[x]$

$\therefore$ closed with respect to multiplication.

(vii) By the definition Associative property is true.

(i.e.,) $P(x)(q(x)R(x)) = (P(x)q(x))R(x)$.

is true.

(viii) By the definition, we can prove

$$P(x)(q(x)+R(x)) = q(x)p(x) + P(x)R(x).$$

$\therefore$ The Distributive law is true.

(ix) Let $p(x)\,q(x) \in F[x]$.

$$\therefore p(x)\,q(x) = c_0 + c_1 x + \cdots + c_t x^t,$$

for each i, $c_i = a_i b_0 + a_{i-1} b_1 + \cdots + a_t b_i$

$$q(x)\,p(x) = d_0 + d_1 x + \cdots + d_t x^t,$$

for each i, $d_i = b_i a_0 + b_{i-1} a_1 + \cdots + b_0 a_i$.

Since F is a Field, $a_i b_0 + a_{i-1} b_1 + \cdots + a_0 b_i$

$$= b_i a_0 + b_{i-1} a_1 + \cdots + b_0 a_i$$

(i.e.,) for each i, $c_i = b_i$

$$\therefore p(x)q(x) = q(x)p(x).$$

$\therefore$ commutative law is true.

(x) Let $p(x) \in F[x]$ $\exists$ $i_1(x) = 1 + 0x + 0x^2 + \cdots + 0x^n \in F[x]$

Such that

$$p(x)\,i_1(x) = (a_0 + a_1 x + \cdots + a_m x^m)(1 + 0x + 0x^2 + \cdots + 0x^n)$$

$$= a_0 + a_1 x + \cdots + a_m x^m.$$

$$= p(x).$$

$$\therefore p(x)\,i_1(x) = p(x).$$

$\therefore 1_{F(x)}$ is the unit element of $F[x]$

$\therefore F[x]$ is a commutative ring with unit element.

4) $D(f)$:

If $f(x) = a_0 + a_1 x + \cdots + a_n x^n \neq 0$ and $a_n \neq 0$.

then the degree of $f(x)$ is n.

It is denoted by $\deg f(x) = n$.

[i.e)] The $\deg f(x)$ is the largest Integer i for which the i^{th} co-efficient of $f(x)$ is not zero].

Note:

A polynomial is a constant if its degree is zero.

Lemma: 3.9.1

If $f(x)\, g(x)$ are two non zero elements of $F[x]$, then $\deg (f(x)g(x)) = \deg f(x) + \deg g(x)$.

Proof:

Suppose that,

$f(x) = a_0 + a_1 x + \cdots + a_m x^m$,

and $g(x) = b_0 + b_1 x + \cdots + b_n x^n$ and $a_m \neq 0$, $b_n \neq 0$ → (1)

$\therefore \deg f(x) = m$ and $\deg g(x) = n$

By the definition,

$f(x)\, g(x) = c_0 + c_1 x + \cdots + c_k x^k$.

where, $c_k = a_k b_0 + a_{k-1} b_1 + \cdots + a_0 b_k$

~~$c_0 = a_0 \cdot b_0$ $c_1 = a_1 \cdot b_1$~~ . . .

We claim that,

$$c_{m+n} = a_m b_n \neq 0$$

and

$$c_i = 0 \quad \forall \; i > m+n.$$

By the definition. Here $t = m+n$

$$c_t = a_t b_0 + a_{t-1} b_1 + \cdots + a_0 b_t$$

$$c_{m+n} = a_{m+n} b_0 + a_{m+n-1} b_1 + \cdots + a_{m+1} b_{n-1} +$$

$$a_m b_n + a_{m-1} b_n + \cdots + a_0 b_{n+m}$$

But from ①,

$$a_{m+1} = a_{m+2} = \cdots = 0$$

$$b_{n+1} = b_{n+2} = \cdots = 0$$

$$\therefore c_{m+n} = (0) b_0 + (0) b_1 + \cdots + (0) b_{n-1} + a_m b_n +$$

$$a_{m-1}(0) + \cdots + a_0 (0)$$

$$\therefore c_{m+n} = a_m b_n \neq 0 \quad \text{— ②} \quad [\text{since } a_m \neq 0,$$

$b_n \neq 0$, $a_m, b_n \in F$

$\therefore a_m b_n \neq 0$].

For $i > m+n$,

$$c_i = a_i b_0 + a_{i-1} b_1 + \cdots + a_0 b_i$$

$$(\text{ie.,}) \quad = \sum_j a_j b_{i-j} \qquad \left.\begin{matrix} j \text{ — ①} \\ i-j \text{ — ②} \end{matrix}\right\} \; j + (i-j).$$

(ie.,) $c_i = \sum_j a_j b_{i-j}$, for every $i > m+n$.

Since $i > m+n$,

$$\Rightarrow j + (i-j) > m+n.$$

$$\Rightarrow j > m \text{ (or) } i-j > n.$$

If $j > m$, then

$$a_j = 0 \Rightarrow a_i b_{i-j} = 0$$

If $i-j > n$, then

$$b_{i-j} = 0 \Rightarrow a_i b_{i-j} = 0$$

In both cases $a_j b_{i-j} = 0$, for $i > m+n$.

$\therefore \sum_j a_j b_{i-j} = 0$ for every $i > m+n$

(ie.,) $c_i = 0$ for every $i > m+n$. → (3)

Thus the highest non zero co-efficient of $f(x)g(x)$ is c_{m+n}.

Hence $\deg (f(x).g(x)) = m+n$.

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

$\therefore \deg (f(x).g(x)) = \deg f(x) + \deg g(x)$.

corollary: 1

If $f(x), g(x)$ are non zero element in $F(x)$, then $\deg f(x) \leq \deg (f(x).g(x))$.

Proof:

We know that, By previous Lemma,

$\deg (f(x).g(x)) = \deg f(x) + \deg g(x)$

Since $g(x)$ is non zero element of $F(x)$,

$\deg g(x) \geq 0$.

$\therefore \deg f(x)g(x) \geq \deg f(x)$

(ie.,) $\deg f(x) \leq (\deg f(x)g(x))$.

corollary: 2

$F[x]$ is an Integral Domain.

Proof:

We know that $F[x]$ is a commutative ring with unit element.

Let $f(x), g(x) \in F[x]$,

$f(x) = a_0 + a_1 x + \cdots + a_m x^m$,

$g(x) = b_0 + b_1 x + \cdots + b_n x^n$, a_i's, b_i's $\in F$

Let $f(x)\,g(x) = 0$.

$\Rightarrow (a_0 + a_1 x + \cdots + a_m x^m)(b_0 + b_1 x + \cdots + b_n x^r)$

$\Rightarrow c_0 + c_1 x + \cdots + c_K x^K = 0$.

where $c_t = a_t b_0 + a_{t-1} b_1 + \cdots + a_0 b_t$

$\Rightarrow c_i = 0$ for all i.

$\Rightarrow a_i b_0 + a_{i-1} b_1 + \cdots + a_0 b_0 = 0$, $\forall i$

$\Rightarrow \sum_j a_j b_{i-j} = 0$, for all i.

$\Rightarrow a_j b_{i-j} = 0$ for all i, j

$\Rightarrow a_j = 0$ (or) $b_{i-j} = 0$ for all i, j

[since $a_i, b_i \in F$, and F is a Field].

$\Rightarrow a_0 + a_1 x + \cdots + a_m x^m = 0$

(or)

$b_0 + b_1 x + \cdots + b_n x^n = 0$.

$\Rightarrow f(x) = 0$ (or) $g(x) = 0$.

$\therefore f(x)\,g(x) = 0$.

$\Rightarrow f(x) = 0$ (or) $g(x) = 0$.

$\therefore F[x]$ has no zero divisors.

$\therefore F[x]$ is an Integral Domain.

Lemma: 3.9.2

The divison Algorithm, given two polynomial $f(x)$ and $g(x) \neq 0$ in $F[x]$. then there exist two polynomials, $t(x)$ $r(x)$ in $F[x]$ such that $f(x) = t(x)g(x) + r(x)$ where $r(x) = 0$ (or) $\deg r(x) < \deg g(x)$.

Proof:

We prove this by Induction on the $\deg f(x)$.

Let $f(x), g(x) \neq 0$ in $F[x]$.

$f(x) = a_0 + a_1 x + \cdots + a_m x^m$ where $a_m \neq 0$.

$g(x) = b_0 + b_1 x + \cdots + b_n x^n$ where $b_n \neq 0$.

$\therefore \deg f(x) = m$ and $\deg g(x) = n$.

Suppose, $m < n$

Then certainly, we have $f(x) = 0\, g(x) + f(x)$

where $\deg f(x) < \deg g(x)$

(or) $f(x) = 0$.

(ie.,) $\exists\ t(x) = 0$ and $r(x) = f(x)$ such that

$f(x) = t(x)g(x) + r(x)$ ——①

where $r(x) = 0$ (or) $\deg r(x) < \deg g(x)$

(ie.,) for $m < n$, the lemma holds.

Now, we prove that $m \geq n$.

Now the lemma holds until $m-1$ ... (assume)

Let $f_1(x) = f(x) - \frac{a_m}{b_n} x^{m-n} g(x)$.

Thus $\deg f_1(x) \leq m-1$.

By Induction hypothesis,

$\exists\, t_1(x), r(x)$ in $F[x]$ such that

$f_1(x) = t_1(x)\, g(x) + r(x)$, where $r(x) \neq 0$, (or)

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

But $f(x) - \frac{a_m}{b_n} x^{m-n} g(x) = t_1(x)\, g(x) + r(x)$

where $r(x) = 0$ (or) $\deg r(x) < \deg g(x)$

$\Rightarrow f(x) = \left[\frac{a_m}{b_n} x^{m-n} g(x)\right] + t_1(x)\, g(x) + r(x)$

$= \left[\frac{a_m}{b_n} x^{m-n} + t_1(x)\right] g(x) + r(x)$

where $r(x) = 0$ (or)

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

If we put $t(x) = \frac{a_m}{b_n} x^{m-n} + t_1 x$,

then

$f(x) = t(x)\, g(x) + r(x)$, where $r(x) = 0$ (or)

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

$t(x), r(x) \in F[x]$.

Thus for every $f(x), g(x) \in F[x]$.

there exist two polynomials $t(x)$ and $r(x) \in F[x]$

such that

$f(x) = t(x)\, g(x) + r(x)$, where $r(x) = 0$ (or)

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

Hence the proof.

Theorem: 3.9.1

$F[x]$ is a Euclidean ring.

Proof:

We know that $F[x]$ is an Integral domain.

To prove:

$F[x]$ is an Euclidean ring.

Define: The function $\deg f(x)$ for all $f(x) \neq 0 \in F[x]$

(i) For $f(x) \neq 0 \in F[x]$,

$\deg(f(x)) \geq 0$.

(ii) By corollary:1,

for all $f(x), g(x) \in F[x]$, not both zero, then

$\deg(f(x)) \leq \deg f(x).g(x)$.

(iii) By Lemma: 3.9.2

For $f(x), g(x) \neq 0 \in F[x]$, $\exists\ t(x), r(x) \in F[x]$

Such that

$f(x) = t(x)g(x) + r(x)$, where $r(x) = 0$ (or)

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

$\therefore F[x]$ is a Euclidean ring.

Lemma: 3.9.3

$F[x]$ is a principle Ideal ring.

Proof:

We know that $F[x]$ is Integral domain.

Let A be an ideal of $F[x]$.

Suppose $a = 0$, then there is nothing to prove.

If $a \neq 0$, then there is an element $a(x) \neq 0 \in F[x]$.

Choose $a_0(x) \in A$ such that

$\deg[a_0(x)]$ is minimal.

Since $a(x), a_0(x) \in F[x]$.

By definition of Euclidean ring

$\exists\ t(x)\ r(x) \in F[x]$ such that,

$$a(x) = t(x)\, a_0(x) + r(x).$$

where $r = 0$ (or) $\deg r(x) < \deg a_0(x)$.

Since $a_0(x) \in A$ and $t(x) \in F[x]$ and A is the Ideal of $F[x]$, then $t(x)\, a_0(x) \in A$.

Since $a(x) \in A$, $t(x)\, a_0(x) \in A$,

$$\Rightarrow a(x) - t(x)\, a_0(x) \in A$$

$$\Rightarrow r(x) \in A.$$

if $r(x) \neq 0$,

then $\deg r(x) < \deg a_0(x)$.

which is a contradiction to our assumption that $\deg(a_0(x))$ is minimal.

$\therefore r(x) = 0$

$\therefore a(x) = t(x)\, a_0(x)$

(ie,) for every $a(x) \neq 0 \in A$.

$\exists\ t(x) \in F(x)$ such that

$$a(x) = t(x) \cdot a_0(x).$$

$\therefore A = (a_0(x))$

$\therefore F[x]$ is a principle Ideal ring.

Lemma: 3.9.4

Given two polynomial $f(x)$, $g(x)$ in $F[x]$ they have a greatest common divisor $d(x)$ which can be realised as $d(x) = \lambda(x) f(x) + \mu(x) g(x)$.

Proof:

Let $A = \{u(x)f(x) + v(x)g(x) / u(x), v(x) \in F[x]\}$

To claim A is an Ideal of $F[x]$.

Let $x, y \in A$

$\therefore x = u_1(x) f(x) + v_1(x) g(x)$

$y = u_2(x) f(x) + v_2(x) g(x)$

Now $x - y = u_1(x) f(x) + v_1(x) g(x) - (u_2(x) f(x) + v_2(x) g(x))$.

$= [u_1(x) - u_2(x)] f(x) + [v_1(x) - v_2(x)] g(x)$.

$\in A$.

$\therefore$ A is a subgroup of $F[x]$ w.r.t addition.

Let $x \in A$, $u(x) \in F[x]$.

$x\,u(x)$; $u(x)\,x$.

$\Rightarrow (u_1(x) f(x) + v_1(x) g(x))\,u(x)$; $u(x)(u_1(x) f(x) + v_1(x) g(x))$.

$\Rightarrow u_1(x) f(x) u(x) + v_1(x) g(x) u(x)$;

$u(x) u_1(x) f(x) + u(x) v_1(x) g(x)$.

$\Rightarrow u_1(x) u(x) f(x) + v_1(x) u(x) g(x)$;

$u(x) u_1(x) f(x) + u(x) v_1(x) g(x) \in A$.

$u_1(x) u(x) f(x) + v_1(x) u(x) g(x) \in A$;

$u(x) u_1(x) f(x) + u(x) v_1(x) g(x) \in A$

$\therefore$ A is an Ideal of $F[x]$.

Since $F[x]$ is an principle Ideal ring,

$A = (d(x))$

(i.e.,) Every element in A is multiple of $d(x)$.

Since $d(x) \in A$ and every element of A is of the form

$$u(x)f(x) + v(x)g(x).$$

$\therefore d(x) = \lambda(x)f(x) + \mu(x)g(x)$ for some $\lambda(x), \mu(x) \in F[x]$

Since $F[x]$ is an Integral domain with unit element,

we can say $1, 0 \in F[x]$.

$\therefore$ we can write $f(x)$ and $g(x)$ as

$$f(x) = 1f(x) + 0g(x) \in A$$

$$g(x) = 0f(x) + g(x) \in A.$$

Since every element in A is a multiple of $d(x)$.

$$d(x) \mid f(x) \quad \text{and} \quad d(x) \mid g(x) \longrightarrow (1)$$

Suppose.

$$c(x) \mid f(x) \text{ and } c(x) \mid g(x)$$

then $c(x) \mid \lambda(x)f(x)$ and $c(x) \mid \mu(x)g(x)$

$$\Rightarrow c(x) \mid \lambda(x)f(x) + \mu(x)g(x).$$

$$\Rightarrow c(x) \mid d(x).$$

$\therefore d(x) \mid f(x)g(x)$.

$\therefore d(x)$ is the greatest common divisor of $f(x)$ and $g(x)$ it form is

$$d(x) = \lambda(x)f(x) + \mu(x)g(x).$$

Def:-

A polynomial $p(x)$ in $F[x]$ is said to be Irreducible over F. if whenever $p(x) = a(x)b(x)$ with $a(x), b(x) \in F[x]$, then one of $a(x)$ (or) $b(x)$ has degree zero [i.e.,) constant].

Example:

Irreducibility depends on the field.

Let us consider the polynomial x^2+1. This is Irreducible over the real field. but not over the complex field.

Since $x^2+1 = (x+i)(x-i)$ where $i^2 = -1$.

Lemma: 3.9.5

Any polynomial in $F[x]$ can be written in a unique manner as a product of irreducible polynomials in $F[x]$.

Proof:

Let $f(x) \in F[x]$.

We prove this by Induction on the deg $f(x)$.

if deg $f(x) = 0$.

then $f(x)$ is a constant polynomial, then there is nothing to prove.

Let deg $f(x) = n$.

Assume that the Lemma is true for all polynomial of degree less than n.

To prove; The Lemma true for the polynomial $F[x]$

Suppose $F[x]$ is Irreducible there is nothing to prove.

Suppose that $f(x) = a(x).b(x)$ where neither deg $(a(x)) = 0$ nor deg $(b(x)) = 0$.

By the corollary of Lemma 3.9.1

deg $f(x) \leq$ deg $f(x)g(x)$

$\therefore \deg(a(x)) < \deg(a(x)b(x)) = \deg f(x) = n$

$\deg(b(x)) < \deg(a(x)b(x)) = \deg f(x) = n.$

$\therefore \deg(a(x)) < n.$

$\deg(b(x)) < n.$

By Induction hypothesis,

$a(x), b(x)$ can be written as the product of Irreducible polynomials.

$\therefore a(x) = a_1(x) + a_2(x) + \cdots + a_m(x)$

$b(x) = b_1(x) + b_2(x) + \cdots + b_n(x).$

where $a_1(x)\ a_2(x) \cdots a_m(x)$,

$b_1(x)\ b_2(x) \cdots b_n(x)$ are Irreducible

polynomial of $F[x]$.

Now,

$f(x) = a(x)b(x)$

$= a_1(x)\ a_2(x) \cdots a_m(x)\ b_1(x) b_2(x) \cdots b_n(x)$

$\geq$ product of Irreducible polynomial of $F[x]$.

$\therefore$ Every element in $F[x]$ can be written as the product of the Irreducible polynomial of $F[x]$.

uniqueness:

Assume that $f(x) = u_1(x)\ u_2(x) \cdots u_m(x)$

$= u_1'(x)\ u_2'(x) \cdots u_n'(x).$

we know that

$u_1(x) \mid u_1(x)\ u_2(x) \cdots u_m(x)$

$\Rightarrow u_1(x) / u_1'(x) u_2'(x) \cdots u_n'(x)$

$\Rightarrow u_1(x) / u_i'(x)$ for some i.

$\Rightarrow u_i'(x) = c_1(x)\, u_1(x)$.

where $c_1(x)$ has degree zero.

Assume that $m < n$.

Thus

$$u_1(x) u_2(x) \cdots u_m(x) = u_1'(x) u_2'(x) \cdots u_{i-1}'(x) \; u_i'(x) u_{i+1}'(x) \cdots u_n'(x)$$

$$u_1(x) u_2(x) \cdots u_m(x) = u_1'(x) u_2'(x) \cdots u_{i-1}'(x)\, c_1(x) u_1(x) \; u_{i+1}'(x) \cdots u_n'(x).$$

$$\therefore u_2(x) u_3(x) \cdots u_m(x) = c_1(x)\, u_1'(x) u_2'(x) \cdots \cdots \; \cdots u_{i-1}'(x) u_{i+1}'(x) \cdots u_n'(x)$$

Repeat the same argument, after m steps product of

$1 = c_1(x) c_2(x) \cdots c_m(x)$ $\quad (n-m$ Irreducible polynomials)

But which is a contradiction.

$\therefore m \geq n$ —— ①

Similarly, we can p.T $n \geq m$ —— ②

From ① & ② we get,

$n = m$.

Hence any polynomial in $F[x]$ can be written as the product of Irreducible polynomial in unique way.

Lemma: 3.9.6

The Ideal $A = (p(x))$ in $F[x]$ is a maximal ideal iff $p(x)$ is Irreducible over f.

Proof:

Let $A = (p(x))$ be a maximal ideal.

we want to p.T

$p(x)$ is Irreducible.

suppose that,

$p(x)$ is not Irreducible, then

$$p(x) = a(x) \cdot b(x).$$

where, neither $\deg a(x) = 0$ nor $\deg b(x) = 0 \longrightarrow (1)$

Let $B = (a(x))$

then $a(x)b(x) = p(x) \in B$ So that $A \subset B$.

Since A is maximal,

either $B = A$ (or) $B = F[x]$

If $B = F[x]$.

then $1 \in F[x] = B$

$\therefore 1 \in B = (a(x))$

$\therefore 1 = \underline{c(x)}\, a(x)$ for some $c(x) \in F[x]$

$\Rightarrow \deg c(x) = 0$ and $\deg a(x) = 0 \longrightarrow (2)$

If $B = A$

Let $a(x) \in B = A = (p(x))$

$\Rightarrow a(x) \in p(x)\underline{u(x)}$. For some $u(x) \in F[x]$.

Now $p(x) = a(x)\, b(x)$

$p(x) = u(x)\, p(x) b(x)$

$1 = u(x)\, b(x)$.

$\Rightarrow \deg u(x) = 0$ and $\deg b(x) = 0 \longrightarrow (3)$

Eq. (2) & (3) gives a contradiction to our Assumption.

$\therefore$ our assumption is wrong.

Hence $p(x)$ is Irreducible.

conversely,

Assume that $p(x)$ is Irreducible.

Let u be an Ideal of $F[x]$ such that

$A = (p(x)) \subset U \subset F[x]$.

Then $U = (u(x))$.

since $p(x) \in A \subset U = (u(x))$

$\therefore p(x) = c(x)\,u(x)$, for some $c(x) \in F[x]$,

but $p(x)$ is Irreducible,

then either $\deg c(x) = 0$ (or) $\deg u(x) = 0$.

If $\deg c(x) = 0$ then $\deg p(x) = \deg u(x)$.

$\Rightarrow A \subset U = (u(x)) \subset (p(x)) = A$.

$\therefore \boxed{A = U}$

If $\deg u(x) = 0$, then $1 \in U$.

Let $f(x) \in F[x]$

W.K.T.

$f(x) \in F[x]$, $1 \in U \Rightarrow 1 \cdot f(x) \in U$

$\Rightarrow f(x) \in U$.

$\therefore f(x) \in F[x] \Rightarrow f(x) \in U$.

$\therefore F(x) \subset U$.

$\therefore \boxed{F(x) = U}$.

(i.e.,) There is no Ideal between A and $F[x]$.

Hence $A = (p(x))$ is the maximal Ideal of $F[x]$.

3.10 polynomial over the rational field.

Def:

The polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$, where $a_0, a_1, a_2, \ldots, a_n$ are Integers, it said to be primitive, if the greatest common divisor of $a_0, a_1, a_2, \ldots, a_n = 1$.

Lemma: 3.10.1

If $f(x)\, g(x)$ are primitive polynomials, then $f(x).g(x)$ is a primitive polynomial.

Proof:

Let $f(x) = a_0 + a_1 x + \cdots + a_m x^m$.

$g(x) = b_0 + b_1 x + \cdots + b_n x^n$.

$f(x).g(x) = c_0 + c_1 x + \cdots + c_t x^t$.

where $c_i = a_i b_0 + a_{i-1} b_1 + \cdots + a_0 b_i$

Suppose that,

$f(x).g(x)$ is not a primitive polynomial, then all the co-efficients of $f(x).g(x)$ would be divisible by some Integer larger than one.

Hence all the co-efficient are divisible by some prime number P.

Since $f(x)$ is primitive, p does not divide some co-efficient a_j.

Let a_j be the first co-efficient of $f(x)$ which p does not divide.

IIIrly, let b_k be the first co-efficient of $g(x)$ which P does not divide.

In $f(x).g(x)$, the co-efficient of x^{j+k} is

$$c_{j+k} = a_{j+k} b_0 + a_{j+k-1} b_1 + \cdots + a_{j+1} b_{k-1} + a_j b_k + a_{j-1} b_{k+1} + \cdots + a_0 b_{k+j}$$

$= a_j b_K + (a_{j+1} b_{K-1} + \cdots + a_{j+K-1} b_1 + a_{j+K} b_0) +$

$(a_{j-1} b_{K+1} + a_{j-2} b_{K+2} + \cdots + a_0 b_{K+j})$ ⟶ ①

Now

by our choice of b_K,

$P / b_{K-1}, b_{K-2}, \ldots$ so that $P / a_{j+1} b_{K-1} + a_{j+2} b_{K-2} + \ldots + a_{j+K} b_0$ ⟶ ②

III^{rly}. by our choice of a_j,

$P / a_{j-1}, a_{j-2}, \ldots$ so that $P / a_{j-1} b_{K+1} + a_{j-2} b_{K+2} + \cdots + a_0 b_{K+j}$ ⟶ ③

By our assumptions,

P / c_{j+K} ⟶ ④

By ①, ②, ③, ④ we get

$P / a_j b_K$ which is a contradiction.

$P \not/ a_j$ and $P \not/ b_K$.

∴ our assumption is wrong.

Hence $f(x) \cdot g(x)$ is a primitive polynomial.

Def:-

The content of the polynomial $f(x) = a_0 + a_1 x + \ldots + a_n x^n$, where a's are Integers, is the greatest common divisor of the Integers $a_0, a_1, \ldots, a_n$.

Note:-

Let $P(x)$ be any polynomial with Integer co-efficients, it can be written as,

$P(x) = d \cdot q(x)$ where d is the constant of $P(x)$

Theorem: 3.10.1

Gauss Lemma.

If the primitive polynomial $f(x)$ can be factored as the product of two polynomial having rational co-efficient, it can be factored as the product of 2 polynomial having Integer's co-efficients.

Proof:

Suppose that $f(x) = u(x) \cdot v(x)$, where $u(x)$ and $v(x)$ have rational co-efficient.

By taking out common vector,

we can write $f(x)$ as

$$f(x) = \frac{a}{b} \lambda(x) \mu(x).$$

where a and b are Integer and where $\lambda(x)$ and $\mu(x)$ have Integer co-efficient and are primitive.

Thus $b \cdot f(x) = a \lambda(x) \mu(x)$ —①

Since $f(x)$ is primitive, the content of the left hand side of ① is b.

Since $\lambda(x) \mu(x)$ are primitive, thenby Lemma 3.10.1 $\lambda(x) \mu(x)$ is primitive, so that the content of the R.H.S of ① is a.

$\therefore a = b$

(i.e.,) $\frac{a}{b} = 1$.

$\therefore f(x) = \lambda(x) \mu(x)$, where $\lambda(x) \mu(x)$ have Integer co-efficient.

Hence the theorem.

Def:

A polynomial is said to be Integer monic if all its co-efficients are Integers and its highest co-efficients is one.

Note:

General form of monic polynomial is,

$x^n + a_1 x^{n-1} + a_2 x^{n-3} + \ldots + a_n$, where a's are Integers.

Clearly an Integer monic polynomial is primitive.

Corollary:

If an Integer monic polynomial factor as the product of two non constant polynomial having the Rational co-efficient, then it factors as the product of two Integers monic polynomials.

Proof:

Let $f(x)$ be an Integer monic polynomials and it can be factors as the product of two non-constant polynomial having rational co-efficient.

Clearly $f(x)$ is primitive.

Then by theorem 3.10.1 [Gauss Lemma], $f(x)$ can be written as the product of two polynomials having Integer co-efficients.

Its $f(x) = \lambda(x)\mu(x)$.

Suppose that $\lambda(x)$ (or) $\mu(x)$ is not a monic polynomial.

Then clearly the product of the two polynomial $\lambda(x)$ and $\mu(x)$.

(ie,) $\lambda(x) \cdot \mu(x)$ is not a monic polynomial.

(ie,) $f(x)$ is not a monic polynomial.

which is a contradiction.

$\therefore f(x) = \lambda(x)\mu(x)$ where $\lambda(x)$ and $\mu(x)$ are Integer monic polynomials.

Hence the theorem.

theorem: 3.10.2 [EISENSTEIN CRITERION].

Let $f(x) = a_0 + a_1(x) + \cdots + a_n x^n$ be a polynomial with Integer co-efficient.

suppose that for some prime number P.

$P \nmid a_n \cdot P \mid P/a_1, P/a_2, \ldots, P/a_0 \cdot P^2 \nmid a_0$.

Then $f(x)$ is Irreducible over the rationals.

Proof:

without loss of Generality we may assume that. if $f(x)$ factored as a product of two rational polynomial, By Gauss Lemma, It factors as the product of two polynomial having Integer co-efficient.

Assume that $f(x)$ is reducible,

then $f(x) = (b_0 + b_1 x + \cdots + b_r x^r)(c_0 + c_1 x + \cdots + c_s x^s)$

where b's and c's are Integers and $r > 0, s > 0$.

(ie.,) $a_0 + a_1 x + \cdots + a_n x^n = (b_0 + b_1 x + \cdots + b_r x^r)$
$(c_0 + c_1 x + \cdots + c_s x^s)$

From this we get $a_0 = b_0 c_0$.

Since $P/a_0 \Rightarrow P/b_0 c_0$; P must divide one of b_0 (or) c_0.

Since $P^2 \nmid a_0$, P cannot divide both b_0 and c_0

Suppose that $P \not| b_0$ but $P \not| c_0$, Not all the co-efficien-
$b_0, b_1, \ldots, b_r$ can be divisible by P.

otherwise, all the co-efficients of $f(x)$ would be divisible by p which is a contradiction to $P \not| a_n$.

Let b_k be the first b not divisible, by P,

$k \leq r < n$. Thus

$P / b_{k-1}, b_{k-2}, \ldots$

but $a_k = b_k c_0 + b_{k-1} c_1 + \ldots + b_0 c_k$.

and $P / a_k, P / b_{k-1}, P / b_{k-2} \ldots$ so that

$P / b_k c_0$ However $P \not| c_0$, $P \not| b_k$, $P / b_k c_0$ is absurd.

$\therefore f(x)$ is Irreducible over rationals.

3.11 polynomial Rings over commutative Rings.

Introduction:

Let R be a commutative ring ~~in~~ with unit element. The polynomial ring in x over R, is denoted by $R[x]$. clearly, $R[x]$ is a commutative ring with unit element.

Let $x_1, x_2, \ldots, x_n$ be n variables over R.

Let $R_1 = R[x_1]$, The polynomial ring in x_1 over R_1

$R_2 = R_1[x_1]$, The polynomial ring in x_2 over R_2

. . . .

. . . .

. . . .

$R_n = R_{n-1}[x_n]$, The polynomial ring in x_n over R_n

Now, R_n is called the ring of polynomials in $x_1, x_2, \ldots, x_n$ over R.

Lemma: 3.11.1

If R is an Integral domain, then so in $R[x]$.

Proof:

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

$f(x) = a_0 + a_1 x + \cdots + a_m x^m$.

$g(x) = b_0 + b_1 x + \cdots + b_n x^n$, $a_0, a_1, \ldots, a_m,$

$b_0, b_1, \ldots, b_n \in R$.

Take,

$f(x)\, g(x) = 0$.

$\Rightarrow (a_0 + a_1 x + \cdots + a_m x^m)(b_0 + b_1 x + \cdots + b_n x^n) = 0$.

$\Rightarrow c_0 + c_1 x + \cdots + c_t x^t = 0$.

$\Rightarrow c_i = 0$ for all i.

$\Rightarrow a_i b_0 + a_{i-1} b_1 + a_{i-2} b_2 + \cdots + a_0 b_i = 0$, for all i.

$\Rightarrow \sum_{j=1}^{i} a_j b_{i-j} = 0$ for all i.

$\Rightarrow a_j b_{i-j} = 0$ for all i, j

$\Rightarrow a_j = 0$ (or) $b_{i-j} = 0$ for all i, j

[$\because R$ is an Integral Domain].

$\Rightarrow a_0 + a_1 x + \cdots + a_m x^m = 0$ (or)

$b_0 + b_1 x + \cdots + b_n x^n = 0$.

$\Rightarrow f(x) = 0$ (or) $g(x) = 0$.

$\therefore R[x]$ is an Integral domain.

Corollary:

If R is an Integral domain, then so is $R[x_1, x_2, \ldots, x_n]$.

Proof:

W.K.T,

$$R_1 = R[x_1]$$

$$R_2 = R_1[x_2] = R[x_1, x_2].$$

$$R_3 = R_2[x_3]$$

$$\vdots$$

$$R_n = R_{n-1}[x_n].$$

Let x_1 be any real number.

Since R is an Integral domain.

By Lemma: 3.11.1

$R_1 = R[x_1]$ is an Integral domain.

Again by Lemma 3.11.1

$R_2 = R_1[x_2]$ is an Integral domain.

Hy, $R_3 = R_2[x_3]$ is an Integral domain.

$$\vdots$$

$R_n = R_{n-1}[x_n]$ is an Integral domain.

(i.e.,) $R[x_1, x_2, \ldots, x_n]$ is an Integral domain.

Def:

Two elements a, b in R are said to be associates if $a = ub$, where u is an unit in R.

An element a which is not a unit if R is called Irreducible, if whenever $a = bc$ with b, c both in R, then one of b (or) c must be ~~until in R~~ a unit in R.

Def:

An Integral domain, R with unit element is a unique factorization domain if,

(a) Any non-zero element in R is either a unit or can be written as the product of a finite number of Irreducible elements of R.

(b) The decomposition in part (a) is unique up to the order and associates of the Irreducible elements..

Lemma: 3.11.2

If R is a unique factorization domains and if a, b are in R, then a and b have a greatest common divisor (a, b) in R. Moreover, if a and b are relatively prime (i.e., (a, b) = 1), whenever a/bc then a/c.

Proof:

Let R be a unique factorisation domain.

Let $a, b \in R$.

case (i):

Let a be a unit in R.

since a is unit then a^{-1} exists.

$\Rightarrow b = a\,a^{-1}b$ [$\because a^{-1}b$ = Integer]

$\Rightarrow a/b$.

$\Rightarrow (a, b) = a$.

IIIrly, if b is a unit element, then $(a, b) = b$

case (ii):

Let a and b are non-units.

Let an Irreducible elements p and q such that

p/a and q/b.

If q is an associate of p, we have,

$q = wp$, for some unit $w \in R$.

then $q/b \Rightarrow p/b$.

If $p \nmid b$ then atleast $1 = p^0/b$.

Let $a = u\, p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$.

$b = v\, p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ for some unit $u, v \in R$.

Any $d/a \Leftrightarrow d = w\, p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$ for some unit w and $0 \le \gamma_i \le \alpha_i$; $1 \le i \le k$.

so, if we assume $\lambda_i = \min(\alpha_i, \beta_i)$ then

$c = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_k^{\lambda_k}$ is a g.c.d of a and b.

(ie.,) $(a, b) = c$ exists.

(ie.,) a and b have a g.c.d in R.

Let $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, $c = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$.

Moreover, Let $(a,b) = 1$ and a/bc.

$\Rightarrow a = \mu_1 p_1^{\mu_1} p_2^{\mu_2} \cdots p_k^{\mu_k}$ where $0 \le \mu_i \le (\beta_i + \gamma_i)$

$= \mu\, p_1^{\beta_1+\gamma_1} p_2^{\beta_2+\gamma_2} \cdots p_k^{\beta_k+\gamma_k}$

$= \mu\, p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$

$\because$ g.c.d $(a,b) = 1$

$\Rightarrow \beta_1 = \beta_2 = \cdots = \beta_k = 0$

$\Rightarrow a_1 = \mu\, p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$

$\Rightarrow a/c$.

corollary:

If $a \in R$ is an Irreducible element and $a|bc$ then $a|b$ (or) $a|c$.

proof:

Given $a \in R$ is an Irreducible element and $a|bc$

suppose $a \nmid b \Rightarrow (a,b) = 1$.

By the lemma, $(a,b) = 1$ and $a|bc \Rightarrow a|c$.

$\therefore a|bc \Rightarrow a|b$ (or) $a|c$.

Lemma: 3.11.3

If R is a unique factorization domain then product of 2 primitive polynomial in $R[x]$ is again a primitive polynomial in $R[x]$.

proof:

Let R be a unique factorization domain.

Let $f(x), g(x) \in R[x]$ be two primitive polynomials over R.

(i.e.,) $f(x) = a_0 + a_1 x + \cdots + a_m x^m$.

$g(x) = b_0 + b_1 x + \cdots + b_n x^n$.

Then $f(x)g(x) = c_0 + c_1 x + \cdots + c_{m+n} x^{m+n}$.

where $c_i = \sum_{j=1}^{i} a_j b_{i-j}$ for $0 \le i \le m+n$.

Suppose that, $f(x)g(x)$ is not primitive polynomial.

Then,

$f(x)g(x)$ would be divisible by some Integer greater than 1.

Let $d = g.c.d\ (c_0, c_1, c_2, \ldots, c_{m+n})$ be a non-unit in R.

There exists an Irreducible element P such that

$P|d$.

clearly, $P \mid c_i$ for every $0 \le i \le m+n$.

since $f(x)$ is primitive, $P \nmid a_i$ for some i.

Let a_j be the first co-efficient of $f(x)$ which

P does not divide.

III^{rly}. b_k be the first co-efficient of $g(x)$ which

P does not divide.

In $f(x)\,g(x)$, the co-efficient of x^{j+k} is

$$c_{j+k} = a_0 b_{j+k} + a_1 b_{j+k-1} + \cdots + a_{j-1} b_{k+1} + a_j b_k + a_{j+1} b_{k-1} + \cdots + a_{j+k} b_0 \longrightarrow (1)$$

Now, our choice of a_j

$P \mid a_{j-1}, a_{j-2}, \ldots$ so that

$P \mid a_{j-1} b_{k+1} + a_{j-2} b_{k+2} + \cdots + a_0 b_{j+k}$

Also, our choice of b_k.

$P \mid b_{k-1}, b_{k-2}, \ldots$ so that

$P \mid a_{j+1} b_{k-1} + a_{j+2} b_{k-2} + \cdots + a_{j+k} b_0$.

$\therefore$ Also $P \mid c_{j+k}$.

$(1) \Rightarrow P \mid a_j b_k$.

$\Rightarrow P \mid a_j$ (or) $P \mid b_k$.

which is a contradiction.

Hence $f(x)\,g(x)$ is primitive.

corollary:

If R is a unique factorization domain and if $f(x) \cdot g(x)$ are in $R[x]$, then $c(fg) = c(f) \cdot c(g)$.

Proof:

Given $f(x)\, g(x) \in R[x]$.

So we can write $f(x) = a f_1(x)$, $a = c(f)$.

$g(x) = b g_1(x)$; $b = c(g)$.

where $f_1(x)$ and $g_1(x)$ are primitive.

Thus $f(x)g(x) = ab\, f_1(x)\, g_1(x)$

Since, the product of primitive polynomial is again primitive,

$f_1(x)\, g_1(x)$ is primitive.

Hence the content of $f(x)\, g(x)$ is ab.

(i.e.,) $c(fg) = ab = c(f)\, c(g)$.

Lemma: 3.11.4

If $f(x)$ in $R[x]$ is both primitive and Irreducible as an element at $R[x]$, then it is Irreducible as an element of $F[x]$. conversely, if the primitive element $f(x)$ in $R[x]$ is Irreducible as an element of $F[x]$, it is also irreducible as an element of $R[x]$

Proof:

Suppose that, the primitive element $f(x)$ in $R[x]$ is Irreducible in $R[x]$, but it reducible in $F[x]$.

Thus $f(x) = g(x)\, h(x)$.

where $g(x), h(x)$ are in $F[x]$ and are of +ve degree.

Now, $g(x) = \dfrac{g_0(x)}{a}$, $h(x) = \dfrac{h_0(x)}{b}$.

where $a, b \in R$ and $g_0(x), h_0(x) \in R[x]$.

Also,

$$g_c(x) = \alpha g_1(x),$$

$$h_c(x) = \beta h_1(x) \quad \text{where } \alpha = c(g_c)$$

$$\beta = c(h_c)$$

and $g_1(x), h_1(x)$ are primitive in $R[x]$.

This $f(x) = \frac{g_c(x)}{a} \cdot \frac{h_c(x)}{b} = \frac{1}{ab} g_c(x) h_c(x)$

$$= \frac{1}{ab} \alpha g_1(x) \beta h_1(x)$$

$$= \frac{\alpha\beta}{ab} g_1(x) h_1(x)$$

$$ab f(x) = \alpha\beta g_1(x) h_1(x) \quad \text{---} (1)$$

Since $g_1(x)$ and $h_1(x)$ are primitive then the product is also primitive.

(i.e.,) $g_1(x) h_1(x)$ is primitive.

Hence the content of R.H.S of (1) is $\alpha\beta$. Since $f(x)$ is primitive, the content of L.H.S is ab.

$\therefore \alpha\beta = ab$.

Hence $f(x) = g_1(x) h_1(x)$.

(ie.,) $f(x)$ are obtain the non-trivial factorization in $R[x]$.

(ie.,) $f(x)$ is reducible in $R[x]$.

which is a contradiction.

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

---

conversely,

Let $f(x)$ be an Irreducible primitive polynomial in $F[x]$.