P.R. GOVT COLLEGE (A)
KAKINADA

GUNNAM PRASADA RAO

LECTURER IN MATHEMATICS

RING THEORY-SEM-IV

INTRODUCTION TO RINGS, SUBRINGS, IDEALS, HOMOMORPHISM, POLYNOMIAL RINGS

UNIT 5: POLYNOMIAL RINGS

Definition: Let R be an arbitary ring and x is called an indeterminate means any symbol but not an element of R. By a polynomial in x over R means an expression of the form

$f(x) = a_0x^0 + a_1x + a_2x^2 + a_3x^3 + \cdots + \infty$

$i.e\ f(x) = \sum_{n=0}^{\infty} a_nx^n$ where $a_0, a_1, a_2, a_3, \ldots$ are elements of $\mathbb{R}$ and only a finite number of them are not zero.

Here $a_0x^0, a_1x, a_2x^2, a_3x^3 \ldots$ are called terms of the polynomials. and

$a_0, a_1, a_2, a_3, \ldots$ are called coefficients of these terms.

Definition: Let R be an arbitary ring and x is an indeterminate. The set of all polynomials $f(x)$,

$f(x) = \sum_{n=0}^{\infty} a_nx^n = a_0x^0 + a_1x + a_2x^2 + a_3x^3 + \cdots + \infty$ is called $R[x]$

$i.e\ \ R[x] =$ The set of all polynomials in x over R

Definition: Let R be an arbitary ring and $f(x), g(x)$ be any two elements in $R[x]$.

Now $f(x) = a_0x^0 + a_1x + a_2x^2 + a_3x^3 + \cdots$ and

$g(x) = b_0x^0 + b_1x + b_2x^2 + b_3x^3 + \cdots$ then

$(i)\ f(x) = g(x) \Leftrightarrow a_n = b_n$ for every non $-$ negative integers.

($i.e$ Two polynomials are equal iff their co $-$ efficient are equal.)

$(ii)\ f(x) + g(x) = \sum_{n=0}^{\infty} c_nx^n = c_0x^0 + c_1x + c_2x^2 + c_3x^3 + \cdots + \infty$ where $c_n = a_n + b_n$

for every non $-$ negative integers.

Since $c_n \in R$ and a finite number of $c's$ can not equal to zero.

$\therefore\ f(x) + g(x)$ is also an element of $R[x]$. Thus $R[x]$ is closed under addition.

$(iii) f(x)g(x) = \sum_{n=0}^{\infty} d_nx^n = d_0x^0 + d_1x + d_2x^2 + d_3x^3 + \cdots + \infty$

$Where\ d_n = a_0b_n + a_1b_{n-1} + a_2b_{n-2} + \cdots + a_nb_0$

$(a_0x^0 + a_1x + a_2x^2 + a_3x^3 + \cdots)(b_0x^0 + b_1x + b_2x^2 + b_3x^3 + \cdots)$

$= (a_0b_0)x^0 + (a_1b_0 + a_0b_1)x + (a_2b_0 + a_1b_1 + a_0b_2)x^2 + \cdots$

$i.e\ d_n = \sum_{i+j=n}^{\infty} a_ib_j\ , inparticular\ d_0 = a_0b_0;\ d_1 = a_1b_0 + a_0b_1;\ d_3 = a_2b_0 + a_1b_1 + a_0b_2$

$Since\ d_n \in R\ and\ a\ finite\ number\ of\ d's\ can\ not\ equal\ to\ zero.$

$\therefore\ f(x)g(x)\ is\ also\ an\ element\ of\ R[x].Thus\ R[x]\ is\ closed\ under\ Multiplication.$

Definition: $A\ polynomial\ f(x) = a_0x^0 + a_1x + a_2x^2 + a_3x^3 + \cdots\ is\ said\ to\ be\ zero$

$polynomial\ if\ foreach\ a_n = 0\ \ \forall\ non - negative\ integers.$

$i.e\ f(x) = 0.x^0 + 0.x + 0.x^2 + 0.x^3 + \cdots$

Degree of polynomial: $A\ polynomial\ f(x) = a_0x^0 + a_1x + a_2x^2 + a_3x^3 + \cdots$

$is\ said\ to\ be\ degree\ n\ if\ a_n \neq 0\ and\ a_m = 0\ \ \forall m > n$

$i.e\ f(x) = a_0x^0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_nx^n\quad if\ a_n \neq 0\ and\ a_m = 0\ \ \forall m > n$

$\therefore a_nx^n\ is\ called\ leading\ term\ of\ f(x)\ and\ a_n\ is\ called\ leading\ coefficient\ of\ f(x)\ and$

$a_0x^0\ is\ called\ constant\ term\ of\ f(x)\ and\ a_0\ is\ called\ \ coefficient\ of zero\ th\ term\ f(x)$

Constant polynomial: $A\ polynomial\ containing\ only\ constant\ term\ is\ called\ constant$

$polynomial.\ Ex: 5x^0$

Note: 1.$The\ degree\ of\ constant\ polynomial\ is\ zero$

2.$The\ degree\ of\ zero\ polynomial\ is\ undefine$

$i.e\ \ 0(x) = 0.x^0 + 0.x + 0.x^2 + 0.x^3 + \cdots$

3.$Degree\ of\big(f(x) + g(x)\big) \leq Maximum\ of\{\ degf(x), \deg(g(x)\}$

$if\ f(x) + g(x)\ are\ not\ zero\ polynomial.$

Example: $f(x) = 3x + 5x^2 - 7x^4\ and\ g(x) = 2x^2 + 5x^3\ are\ two\ polynomial$

$over\ the\ ring\ of\ integers.$

$Now\ f(x) + g(x) = 3x + 7x^2 + 5x^3 - 7x^4$

$So\ deg\{f(x)+g(x)\}=4=\deg of g(x)$

$4.\ f(x)g(x)=(3x+5x^2-7x^4)(2x^2+5x^3)=6x^3+10x^4-14x^6+15x^4+25x^5-35x^7$

$=6x^3+25x^4+25x^5-14x^6-35x^7$

$i.e\ \deg\{f(x).g(x)\}=7\leq \deg of\ f(x)+\deg of g(x)$

$if\ f(x).g(x)\ are\ not\ zero\ polynomial.$

***Theorem*: *If R is an integraldomain so is R*[*x*]**

***Proof*:** $R[x]=The\ set\ of\ all\ polynomials\ in\ x\ over\ R.$

$Let\ f(x)=a_0x^0+a_1x+a_2x^2+a_3x^3+\cdots+a_mx^m+\cdots$

$g(x)=b_0x^0+b_1x+b_2x^2+b_3x^3+\cdots+b_nx^n+\cdots$

$h(x)=c_0x^0+c_1x+c_2x^2+c_3x^3+\cdots+c_px^p+\cdots\ \ be\ three\ elements\ in\ R[x]$

$so\ that\ a_i=0\ \forall\ i>m,\qquad b_j=0\ \forall\ j>n, c_k=0\ \forall\ k>p$

(*i*) + *is a binary operation on R*[*x*]:

$Let\ r=Max\{m,n\}\ then\ a_t=0\ for\ t>r\ and\ b_t=0\ for\ t>r$

$\therefore\ a_t+b_t=0\ \ \forall\ t>r$

$\therefore f(x)+g(x)=(a_0+b_0)x^0+(a_1+b_1)x+(a_2+b_2)x^2+\cdots+(a_r+b_r)x^r+\cdots$

$So\ that\ \ a_t+b_t=0\ \ \forall\ t>r$

$By\ definition\ of\ the\ polynomial\ f(x)+g(x)\in R[x]$

(*ii*) · *is binary operation on R*[*x*]:

$If\ l>m+n\ then\ i+j=l\ \ when\ either\ i>m\ or\ j>n\ so\ a_ib_j=0\ \ \forall i+j>m+n$

$\therefore f(x)g(x)=d_0x^0+d_1x+d_2x^2+\cdots+d_{m+n}x^{m+n}+\cdots\ \ where\ d_{m+n}=\sum_{i+j=m+n}^{\infty}a_ib_j$

$so\ that\ d_l=0\ \ \forall\ l>m+n$

$\therefore By\ definition\ of\ polynomial\ f(x)g(x)\in R[x]$

$\therefore R[x]\ is\ closed\ under\ multiplication.$

(iii) $+$ *is commutative*:

$f(x)+g(x)=(a_0+b_0)x^0+(a_1+b_1)x+(a_2+b_2)x^2+\cdots$ $(\because$ $+$ *is commutative in* $\mathbb{R})$

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

(iv) $+$ *is associative*:

$[f(x)+g(x)]+h(x)$

$=[(a_0+b_0)+c_0]x^0+[(a_1+b_1)+c_1]x+[(a_2+b_2)+c_2]x^2+\cdots$

$(\because$ $+$ *is commutative in* $\mathbb{R})$

$=[a_0+(b_0+c_0)]x^0+[a_1+(b_1+c_1)]x+[a_2+(b_2+c_2)]x^2+\cdots$

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

(v) *Existanceof additive identity* (or) *Zero elementof* $R[x]$: *For* $0\in R$,

$0(x)=0.x^0+0.x+0.x^2+0.x^3+\cdots\in R[x]$

For any $f(x)\in R[x]$,

$f(x)+0(x)=(a_0+0)x^0+(a_1+0)x+(a_2+0)x^2+\cdots$

$=a_0x^0+a_1x+a_2x^2+a_3x^3+\cdots=f(x)$

Since $+$ *is commutative,* $\quad f(x)+0(x)=f(x)=0(x)+f(x)$

$\therefore 0(x)=0.x^0+0.x+0.x^2+0.x^3+\cdots$ *is the zero element of* $R[x]$

(vi) *Existanceof additive inverse*:

Let $f(x)=a_0x^0+a_1x+a_2x^2+a_3x^3+\cdots\in R[x]$ *Then* $a_0,a_1,a_2,a_3,\ldots\in R$

since R is aring so we have $-a_0,-a_1,-a_2,-a_3,\ldots\in R$

$\Longrightarrow(-a_0)x^0+(-a_1)x+(-a_2)x^2+(-a_3)x^3+\cdots\in R[x]$ *say* $f^1(x)$

Now $f(x)+f^1(x)=[a_0+(-a_0)]x^0+[a_1+(-a_1)]x+[a_2+(-a_2)]x^2+\cdots$

$=0.x^0+0.x+0.x^2+0.x^3+\cdots=0(x)$

Since $+$ *is commutative,* $\quad f(x)+f^1(x)=0(x)=f^1(x)+f(x)$

$\therefore$ $f^1(x)$ *is additive inverse of* $f(x)$

$\therefore$ *Every element of* $R[x]$ *has inverse in* $R[x]$

(vii) · is an associative:

$f(x)g(x) = (a_0x^0 + a_1x + a_2x^2 + a_3x^3 + \cdots)(b_0x^0 + b_1x + b_2x^2 + b_3x^3 + \cdots)$

$= d_0x^0 + d_1x + d_2x^2 + \cdots + d_sx^s + \cdots \ \ where\ d_s = \sum_{i+j=s}^{\infty} a_ib_j$

$[f(x)g(x)]h(x) = (d_0x^0 + d_1x + d_2x^2 + \cdots + d_sx^s + \cdots)(c_0x^0 + c_1x + c_2x^2 + c_3x^3 + \cdots)$

$= e_0x^0 + e_1x + e_2x^2 + e_3x^3 + \cdots + e_tx^t + \cdots$

Where e_t *is the coefficient of* x^t *in* $[(f(x)g(x)]$

$$e_t = \sum_{t=s+k}^{\infty} d_sc_k \Longrightarrow e_t = \sum_{t=s+k}^{\infty} \left(\sum_{i+j=s}^{\infty} a_ib_j \right) c_k = \sum_{t=i+j+k}^{\infty} a_ib_jc_k$$

Similarly we can prove that the coefficient of x^t *in* $f(x)[g(x)h(x)]$ *is* $\sum_{t=i+j+k}^{\infty} a_ib_jc_k$

$\therefore [f(x)g(x)]h(x) = f(x)[g(x)h(x)]$

Since the corresponding coefficients in these two polynomials are equal.

(viii) · is distributive under addition: *Let t be any non − negative integer.*

$$The\ coefficient\ of\ x^t\ in\ f(x) \cdot [g(x) + h(x)] = \sum_{t=i+j}^{\infty} a_i \cdot (b_j + c_j) = \sum_{t=i+j}^{\infty} (a_i \cdot b_j + a_i \cdot c_j)$$

$$= \sum_{t=i+j}^{\infty} a_i \cdot b_j + \sum_{t=i+j}^{\infty} a_i \cdot c_j$$

$= The\ coefficient\ of\ x^t\ in\ f(x) \cdot g(x) + The\ coefficient\ of\ x^t\ in\ f(x) \cdot h(x)$

$\therefore f(x) \cdot [g(x) + h(x)] = f(x) \cdot g(x) + f(x) \cdot h(x)$

Since the corresponding coefficients in these two polynomials are equal.

Similarly we can prove that $[g(x) + h(x)] \cdot f(x) = g(x) \cdot f(x) + h(x) \cdot f(x)$

$\therefore (R[x], +, \cdot)$ *is ring*

(ix) · is commutative: *Let t be any non − negative integer.*

$$The\ coefficient\ of\ x^t\ in\ f(x)\cdot g(x) = \sum_{t=i+j}^{\infty} a_i \cdot b_j = \sum_{t=j+i}^{\infty} b_j \cdot a_i \quad (\because \cdot\ is\ commutative)$$

$$= The\ coefficient\ of\ x^t\ in\ g(x)\cdot f(x)$$

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

Since the corresponding coefficients in these two polynomials are equal.

$$\therefore (R[x], +, \cdot)\ is\ commutative\ ring$$

(x) $R[x]$ has no zero divisors:

$$Let\ f(x) = a_0x^0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_mx^m + \cdots, \quad a_m \neq 0$$

$$g(x) = b_0x^0 + b_1x + b_2x^2 + b_3x^3 + \cdots + b_nx^n + \cdots, \quad b_n \neq 0\ be\ two$$

$$non - zero\ elements\ in\ R[x]$$

$$Then\ f(x)g(x)\ can\ not\ be\ a\ zero\ polynomial.\ i.e\ zero\ element\ of\ R[x].$$

$$The\ reason\ is\ that\ at\ least\ one\ coefficient\ of\ f(x)g(x)\ namely\ a_mb_n\ of\ x^{m+n} \neq 0,$$

$$because\ a_m, b_n \in R\ and\ R\ has\ nozero\ divisors$$

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

$$\therefore (R[x], +, \cdot)\ is\ integral\ domain.$$

Theorem 2: ***If R is commutative ring with unity so is $R[x]$***

Proof: *Write the proof of above theorem from i to ix steps*

(x) $R[x]$ has unity element: $If\ 1 \in R\ is\ the\ unity\ element\ then$

$$1(x) = 1\cdot x^0 + 0.x + 0.x^2 + 0.x^3 + \cdots \in R[x]$$

$$Let\ f(x) = a_0x^0 + a_1x + a_2x^2 + a_3x^3 + \cdots be\ any\ element\ of\ R[x]$$

$$Now\ \ f(x)\cdot 1(x) = (a_0\cdot 1)x^0 + (a_1\cdot 1 + 0)x + (a_2\cdot 1 + 0)x^2 + \cdots$$

$$= a_0x^0 + a_1x + a_2x^2 + a_3x^3 + \cdots = f(x)$$

$$Since\ \cdot\ is\ commutative$$

$$f(x)\cdot 1(x) = 1(x)\cdot f(x) = f(x)$$

$$\therefore 1(x)\ is\ the\ unity\ element\ in \in R[x]$$

Note: *Let $f(x)$ and $g(x)$ be two non − zero polynomials in $R[x]$then*

(i)Degree of $[f(x)+g(x)] \leq$ Max of $\{degf(x), degg(x)\}$ if $f(x)+g(x)$ is not a zero polynomials

(ii)Degree of $[f(x)\cdot g(x)] \leq degf(x) + degg(x)$ if $f(x)\cdot g(x)$ is not a zero polynomials

(iii) If $f(x)$ is any polynomialin $R[x]$ then $f(x)\cdot 0(x) = 0(x)$

(iv) If R is an Integral domain and $f(x), g(x)$ be two non − zero polynomials in $R[x]$ then deg of $[f(x)\cdot g(x)] = degf(x) + degg(x)$ if $f(x)\cdot g(x)$ is not a zero polynomials

(v) If R is field and $f(x), g(x)$ be two non − zero polynomials in $R[x]$ then deg of $[f(x)\cdot g(x)] = degf(x) + degg(x)$ if $f(x)\cdot g(x)$ is not a zero polynomials ($\because$ Every fieldis an integral domain)

Theorem 3: ***If F is a field then $F[x]$ is an integral domain but not a field***

Proof: *Write the proof of theorem* 1

Let $f(x)$ be any polynomial in $F[x]$ of degree greater than zero.

The inverse of $f(x)$ is not a zero polynomial because the product of $f(x)$and zero polynomial is zero polynomial{$i.e\ f(x)\cdot 0(x) = 0(x)$}

and is not equal to unity element of $F[x]$($1(x) = 1\cdot x^0 + 0.x + 0.x^2 + 0.x^3 + \cdots$

Suppose $g(x)$ is any non − zero polynomial in $F[x]$.

Since F is afield,

Now deg *of $[f(x)\cdot g(x)] = degf(x) + degg(x) > 0$ ($\because degf(x) > 0$ and $degg(x) \geq 0$)*

Since degree of unity element is zero, $f(x)\cdot g(x)$ can not be equal to unity element of $F[x]$

$\therefore$ $f(x)$ has no inverse in $F[x]$

Theorem 4(Division algorithm for polynomials): *Let F be a field. For any $f(x), g(x) \in F[x]$ and $g(x) \neq 0(x)$ then there exists unique polynomials $q(x), r(x) \in F[x]$ such that $f(x) = g(x)q(x) + r(x)$ Where $r(x) = 0(x)$ or $degr(x) < degg(x)$*

Proof: *Consider the set* $S = \{f(x) - g(x)h(x)/h(x) \in F[x]\}$

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

$f(x) - g(x) \cdot 0(x) = f(x) - 0(x) = f(x) \in S \Longrightarrow S \neq \emptyset$ *and* $S \subseteq F[x]$

Let $0(x) \in S$, *By the definition of* S, $\exists\, q(x) \in F[x]$ *suchthat*

$0(x) = f(x) - g(x) \cdot q(x) \Longrightarrow f(x) = g(x) \cdot q(x) + 0(x)$

$\Longrightarrow f(x) = g(x) \cdot q(x) + r(x)$ *Where* $r(x) = 0(x) \in F[x]$

The theorem is proved.

Let $0(x) \notin S$

Then all the polynomials in S are non − zero polynomilas and hence non − negative degree.

Let $r(x) \in S$ *be a polynomial of least degree*

By the def *of* $S, \exists\ q(x) \in F[x]$ *suchthat* $r(x) = f(x) - g(x)q(x)$

$\Longrightarrow f(x) = g(x)q(x) + r(x) \longrightarrow (1)$

Now we showthat $degr(x) < degg(x)$.

Let $g(x) = a_0x^0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + a_nx^n + \cdots$ *where* $a_n \neq 0$ *be a polynomial so that* $degg(x) = n$

.If possible suppose $m = degr(x) \geq degg(x)$

Let $r(x) = c_0x^0 + c_1x + c_2x^2 + \cdots + c_{m-1}x^{m-1} + c_mx^m + \cdots$ *where* $c_m \neq 0$ *be a polynomial*

Now $c_m a_n^{-1} x^{m-n} g(x) = c_m a_n^{-1} a_0 x^{m-n} + c_m a_n^{-1} a_1 x^{m-n+1} + \cdots + c_m a_n^{-1} a_n x^{m-n+n}$

$c_m a_n^{-1} x^{m-n} g(x) = c_m a_n^{-1} a_0 x^{m-n} + c_m a_n^{-1} a_1 x^{m-n+1} + \cdots + c_m x^m$

$\therefore r(x) = c_0x^0 + c_1x + c_2x^2 + \cdots + c_{m-1}x^{m-1} + c_mx^m + \cdots$

$$\Longrightarrow r(x) = c_0x^0 + c_1x + c_2x^2 + \cdots + c_{m-1}x^{m-1} + [c_m a_n^{-1}x^{m-n}g(x) - c_m a_n^{-1}a_0x^{m-n} - c_m a_n^{-1}a_1x^{m-n+1} - \cdots - c_m a_n^{-1}a_{n-1}x^{m-1}]$$

$$\Longrightarrow r(x) = c_m a_n^{-1}x^{m-n}g(x) + (c_{m-1} - c_m a_n^{-1}a_{n-1})x^{m-1} + \cdots + c_1x + c_2x^2 + c_0x^0$$

$$\Longrightarrow r(x) = c_m a_n^{-1}x^{m-n}g(x) + \alpha(x) \longrightarrow (2)$$

$Where\ \alpha(x) = (c_{m-1} - c_m a_n^{-1}a_{n-1})x^{m-1} + \cdots + c_1x + c_2x^2 + c_0x^0$

$\therefore deg\alpha(x) \leq m-1 \Longrightarrow deg\alpha(x) < m \Longrightarrow deg\alpha(x) < degr(x)$

$From\ (1)\ \&\ (2)$

$$f(x) = g(x)q(x) + c_m a_n^{-1}x^{m-n}g(x) + \alpha(x)$$

$$\Longrightarrow f(x) = g(x)[q(x) + c_m a_n^{-1}x^{m-n}] + \alpha(x)$$

$$\Longrightarrow \alpha(x) = f(x) - g(x)\beta(x) \quad Where\ \beta(x) = q(x) + c_m a_n^{-1}x^{m-n} \in F[x]$$

$\Longrightarrow \alpha(x) \in S$

$Thus\ \alpha(x) \in S\ and\ deg\alpha(x) < degr(x)$

$Which\ is\ a\ contradiction\ to\ degr(x)\ to\ be\ the\ least.$

$\therefore Our\ supposition\ is\ wrong.$

$Hence\ degr(x) < degg(x)$

$Thus\ there\ exists\ q(x), r(x) \in F[x]\ sothat\ f(x) = g(x)q(x) + r(x)$

$Where\ r(x) = 0(x)\ \ or\ degr(x) < degg(x)$

Uniqueness of $q(x), r(x)$: $If\ possible\ suppose\ that\ q^1(x), r^1(x) \in F[x]\ so\ that$

$$f(x) = g(x)q^1(x) + r^1(x) \quad where\ r^1(x) = 0(x)\ or\ degr^1(x) < degg(x)$$

$$\therefore g(x)q(x) + r(x) = g(x)q^1(x) + r^1(x) \Longrightarrow g(x)[q(x) - q^1(x)] = r^1(x) - r(x)$$

$$If\ q(x) - q^1(x) \neq 0(x)\ \ then\ deg(g(x)\cdot[q(x) - q^1(x)]) = degg(x) + \deg(q(x) - q^1(x)]$$

$[Since\ F[x]\ is\ an\ I.D, g(x) \neq o(x), q(x) - q^1(x) \neq 0(x) \Longrightarrow g(x)[q(x) - q^1(x)] \neq 0(x)]$

$$\therefore \deg[r^1(x) - r(x)] = degg(x) + \deg(q(x) - q^1(x)]$$

$$\Longrightarrow \deg[r^1(x) - r(x)] \geq degg(x)$$

$Which\ is\ a\ contradiction\ to\ degr(x) < degg(x), degr^1(x) < degg(x)$

$\therefore q(x) - q^1(x) = 0(x)\ and\ r^1(x) - r(x) = 0(x)$

$\Longrightarrow q(x) = q^1(x)\ and\ r^1(x) = r(x)$

***Theorem 5**: If F is a field then F[x] is principal ideal domian.*

***Proof**: Since F is a field*

$F[x] = The\ set\ of\ all\ polynomials\ in\ x\ over\ F.$

$\therefore F[x]\ is\ an\ integral\ domain.$

$Let\ I\ be\ any\ ideal\ of\ F[x].$

$Let\ I = \{0(x)\}\ where\ 0(x)\ is\ the\ zero\ element\ of\ F[x]$

$Then\ I =< 0(x) >\ is\ the\ ideal\ generated\ by\ 0(x)$

$\therefore I\ is\ a\ principal\ ideal.$

$Let\ I \neq \{0(x)\}\ so\ there\ exists\ g(x) \neq 0(x) \in I\ so\ that\ the\ set\ \{degg(x)/g(x) \neq 0(x)\}\ is$

$non - negative\ integers.$

$By\ the\ well\ ordering\ principal\ \exists\ f(x) \neq 0(x) \in I\ so\ that\ degf(x) \leq degg(x)$

$for\ g(x) \neq 0(x) \in I$

$To\ prove\ that\ I =< f(x) >$

$Let\ h(x)\ be\ any\ element\ of\ I$

$By\ division\ algorithm\ for\ polynomials\ so\ \exists unique\ q(x), r(x) \in F[x] so\ that$

$h(x) = f(x)q(x) + r(x)\ \ where\ \ r(x) = 0(x)\ or\ degr(x) < degf(x)$

$Since\ f(x) \in I, q(x) \in F[x]\ and\ I\ is\ an\ ideal\ \Longrightarrow f(x)q(x) \in I$

$Since\ h(x) \in I, f(x)q(x) \in I\ and\ I\ is\ an\ ideal \Longrightarrow h(x) - f(x)q(x) \in I$

$\Longrightarrow h(x) - f(x)q(x) = r(x) \in I \Longrightarrow r(x) \in I$

$Since\ r(x) \in Iand\ r(x) = 0(x)\ or\ degr(x) < degf(x)$

$If\ r(x) \in I\ and\ r(x) \neq 0(x)\ then\ degr(x) < degf(x)$

$Which\ is\ a\ contradiction\ to\ degf(x)\ is\ the\ least. \therefore r(x) = 0(x)$

$\therefore h(x) = f(x)q(x) + 0(x)\ \ forsome\ q(x) \in F[x]$

$\therefore I = \{f(x)q(x)/q(x) \in F[x]\}$

$I =< f(x) > is\ a\ principal\ ideal.$

$\therefore Every\ ideal\ is\ a\ principal\ ideal.$

$\therefore F[x]\ is\ a\ principal\ ideal\ domain.$

Problems

1. *Find the sum and product of the polynomial* $\boldsymbol{f(x) = 2 + 3x - 4x^2 + 5x^3}$,

$\boldsymbol{g(x) = 5 - 2x + 3x^2 - 2x^3 + 2x^4}$ ***over*** $\mathbb{Z}$

Sol: $f(x) = 2 + 3x - 4x^2 + 5x^3, g(x) = 5 - 2x + 3x^2 - 2x^3 + 2x^4$

$f(x) + g(x) = (2 + 3x - 4x^2 + 5x^3) + (5 - 2x + 3x^2 - 2x^3 + 2x^4)$

$= 7 + x - x^2 + 3x^3 + 2x^4$

$f(x) \cdot g(x) = (2 + 3x - 4x^2 + 5x^3) \cdot (5 - 2x + 3x^2 - 2x^3 + 2x^4)$

$= 10 + (-4 + 15)x + (6 - 6 - 20)x^2 + (-4 + 9 + 8 + 25)x^3 + (4 - 6 - 12 - 10)x^4$
$+ (6 + 8 + 15)x^5 + (-8 - 10)x^6 + 10x^7$

$= 10 + 11x - 20x^2 + 38x^3 - 24x^4 + 29x^5 - 18x^6 + 10x^7$

2. *Find the sum and product of all the polynomials* $\boldsymbol{f(x) = 2 + 3x + 5x^2, g(x)}$
$\boldsymbol{= 1 + 2x + 3x^2}$ ***over*** $\boldsymbol{Z_6}$

Sol: $f(x) = 2 + 3x + 5x^2, g(x) = 1 + 2x + 3x^2\ over\ Z_6$

$f(x) + g(x) = (2 + 3x + 5x^2) + (1 + 2x + 3x^2) = (2 +_6 1) + (3 +_6 2)x + (5 +_6 3)x^2$

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

$f(x) \cdot g(x) = (2 + 3x + 5x^2) \cdot (1 + 2x + 3x^2)$

$= (1 \times_6 2) + [(1 \times_6 3) + (2 \times_6 2)]x + [(1 \times_6 5) + (2 \times_6 3) + (3 \times_6 2)]x^2$

$+[(3 \times_6 3) + (2 \times_6 5)]x^3 + (3 \times_6 5)x^4 = 2 + x + 5x^2 + x^3 + 3x^4$

3. *Find the sum and product of all the polynomials* $\boldsymbol{f(x) = 2 + 3x + 4x^2, g(x)}$
$\boldsymbol{= 4 + 2x + 3x^4}$ ***over*** $\boldsymbol{Z_5}$

Irreducible polynomials: *Let* F *be a field. A non* $-$ *constant polynomial* $f(x) \in F[x]$

is said to be irreducible polynomialover F *if* $f(x)$ *cannot be expressed as the product of two*

$polynomials\ of\ lower\ degree\ thant\ he\ degree\ of\ f(x).$

$i.e\ f(x) \neq g(x)h(x)$

Problems

1. $f(x) = x^2 + 1$ is irreducible over the field of $\mathbb{R}$ but it is reducible over $\mathbb{C}$

Sol: $f(x) = x^2 + 1 = (x + i)(x - i)\ is\ reducible\ over\ \mathbb{C}$

$but x^2 + 1 = (x + i)(x - i)\ where\ i \notin \mathbb{R}\ is\ irreducible\ over\ the\ field\ of\ \mathbb{R}$

2. $f(x) = x^2 - 2$ is irreducible over the field of $\mathbb{Q}$ but it is reducible over $\mathbb{R}$

Sol: $f(x) = x^2 - 2 = \left(x + \sqrt{2}\right)\left(x - \sqrt{2}\right)\ is\ irreducible\ over\ \mathbb{Q}$

$but\ x^2 + 1 = \left(x + \sqrt{2}\right)\left(x - \sqrt{2}\right)\ where \sqrt{2} \in \mathbb{R}\ is\ reducible\ over\ the\ field\ of\ \mathbb{R}$

Eisenstien criteria: $Let\ f(x) = a_0x^0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + a_nx^n \in \mathbb{Z}[x],$

$n \geq 1. If\ there\ is\ a\ prime\ p\ such\ that\ p/a_0\ , p/a_1\ , \ldots p/a_{n-1}\ , p \nmid a_n\ and\ p^2 \nmid a_0\ then$

$f(x)\ is\ irreducible\ over\ \mathbb{Q}.$

Proof: $Given\ that f(x) = a_0x^0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + a_nx^n \in \mathbb{Z}[x],$

$n \geq 1$

$Assume\ that\ there\ exist\ a\ prime\ p\ such\ that\ \ p/a_0\ , p/a_1\ , \ldots p/a_{n-1}\ , p \nmid a_n\ and\ p^2 \nmid a_0.$

$If\ possible\ suppose\ that\ f(x)\ is\ reducible\ over\ \mathbb{Q}.$

$By\ using\ definition\ of\ reducible\ polynomial$

$f(x) = (b_0x^0 + b_1x + b_2x^2 + \cdots + b_rx^r)(c_0x^0 + c_1x + c_2x^2 + \cdots + c_sx^s)$

$Where\ b_i, c_i \in \mathbb{Z}\ and\ r < n\ and\ s < n\ and\ r + s = n$

$Compare\ the\ coefficient\ on\ both\ side\ we\ get\ a_0 = b_0c_0, \ldots ,\qquad a_n = b_rc_s$

$By\ hyp; p^2 \nmid a_0\ and\ \ p \nmid a_n \Longrightarrow p^2 \nmid b_0c_0\ and\ \ p \nmid b_rc_s \longrightarrow (1)$

$But\ it\ is\ given\ that\ p^2 \nmid a_0\ and\ \ p/a_0 \Longrightarrow p^2 \nmid b_0c_0\ and\ p/b_0c_0$

$(suppose\ that\ p/b_0c_0 \Longrightarrow\ p/b_0 and\ \ p/c_0$

$\Longrightarrow b_0 = pm; and\ c_0 = pl\ \ for some\ m, l \in \mathbb{Z}$

$Now\ \ b_0c_0 = (pm)(pl) = p^2lm \Longrightarrow b_0c_0 = p^2n\ \ where\ \ n = lm \in \mathbb{Z} \Longrightarrow p^2/b_0c_0 \Longrightarrow p^2/a_0$

$Which\ is\ contradiction\ to\ p^2 \nmid a_0. So\ p/b_0c_0\ \ is\ not\ possible$

$\therefore p^2 \nmid b_0c_0 \Longrightarrow either\ \ p/c_0\ \ and\ p \nmid b_0\ \ or\ \ \ p \nmid c_0\ and\ p/b_0$

$Here\ we\ consider\ the\ p/c_0\ \ and\ p \nmid b_0$

$From(1)\ \ p \nmid b_rc_s \Longrightarrow p \nmid b_r\ \ \ and\ \ p \nmid c_s$

$Let\ c_m\ be\ the\ first\ coefficient\ of\ s\ in\ c_0x^0 + c_1x + c_2x^2 + \cdots c_mx^m + \cdots + c_sx^s\ such\ that$

$p \nmid c_m \Longrightarrow p \nmid a_m because\ p/a_m \Longrightarrow p/c_m\ \ since\ a_m = combination\ of\ c_m and\ b_m$

$a_m = a_n\ \ (\because p \nmid a_n) \Longrightarrow m = n$

$p \nmid c_m \Longrightarrow p \nmid c_s(last\ term) \Longrightarrow m \leq s \Longrightarrow m \leq s < n \Longrightarrow n = m \leq s < n \Longrightarrow n \leq s < n$

$\Longrightarrow n < n\ Which\ is\ a\ contradiction.$

$Similarly\ the\ same\ absurdity\ happen\ in\ case\ p \nmid c_0\ and\ p/b_0$

$\Longrightarrow In\ both\ cases\ we\ get\ contradiction \Longrightarrow Our\ assumption\ was\ wrong.$

$\Longrightarrow f(x)\ should\ be\ irreducible\ over\ \mathbb{Q}$

Problems

1. Show that $f(x) = x^2 - 2$ is irreducible over $\mathbb{Q}$

Sol: $f(x) = -2 + 0 \cdot x + x^2 \in \mathbb{Z}[x]\ \ \ Here\ a_0 = -2\ , a_1 = 0, a_2 = 1$

$Take\ least\ prime, p = 2; 2/-2 \Longrightarrow p/a_0; 2/0 \Longrightarrow p/a_1, 2 \nmid 1 \Longrightarrow p \nmid a_2$

$p^2 = 4\ and\ 4 \nmid -2 \Longrightarrow p^2 \nmid a_0$

$By\ Eisenstein\ criterion\ f(x) = x^2 - 2\ is\ irreducible\ over\ \mathbb{Q}$

2. Show that $f(x) = x^4 + 2x + 2$ is irreducible over $\mathbb{Q}$

Sol: $f(x) = 2 + 2x + 0.x^2 + 0.x^3 + x^4 \in \mathbb{Z}[x]\ \ \ Here\ a_0 = 2\ , a_1 = 2, a_2 = 0, a_3 = 0, a_4 = 1$

$Take\ least\ prime, p = 2;\ \ 2/2 \Longrightarrow p/a_0; 2/2 \Longrightarrow p/a_1, 2/0 \Longrightarrow p/a_2,$

$2/0 \Longrightarrow p/a_3, 2 \nmid 1 \Longrightarrow p \nmid a_4$

$p^2 = 4\ and\ 4 \nmid 2 \Longrightarrow p^2 \nmid a_0$

$By\ Eisenstein\ criterion\ f(x) = x^4 + 2x + 2\ is\ irreducible\ over\ \mathbb{Q}$

3. *Show that $f(x) = 25x^5 - 9x^4 + 3x^2 - 12$ is irreducible over $\mathbb{Q}$*

Sol: $f(x) = -12 + 0.x + 3x^2 + 0.x^3 - 9x^4 + 25x^5 \in \mathbb{Z}[x]$

Here $a_0 = -12\,, a_1 = 0, a_2 = 3, a_3 = 0, a_4 = -9, a_5 = 25$

Take $p = 3;\quad 3/-12 \Longrightarrow p/a_0; 3/0 \Longrightarrow p/a_1, 3/3 \Longrightarrow p/a_2,$

$3/0 \Longrightarrow p/a_3, 3/-9 \Longrightarrow p/a_4, 3 \nmid 25 \Longrightarrow p \nmid a_5$

$p^2 = 9$ *and* $9 \nmid -12 \Longrightarrow p^2 \nmid a_0$

By Eisenstein criterion $f(x) = 25x^5 - 9x^4 + 3x^2 - 12$ *is irreducible over* $\mathbb{Q}$

4. *Show that $f(x) = 8x^3 + 6x^2 - 9x + 24$ is irreducible over $\mathbb{Q}$*

Sol: $f(x) = 24 - 9x + 6x^2 + 8x^3 \in \mathbb{Z}[x]$

Here $a_0 = 24\,, a_1 = -9, a_2 = 6, a_3 = 8,$

Take $p = 3;\quad 3/24 \Longrightarrow p/a_0; 3/-9 \Longrightarrow p/a_1, 3/6 \Longrightarrow p/a_2,$

$3 \nmid 8 \Longrightarrow p \nmid a_5$

$p^2 = 9$ *and* $9 \nmid 24 \Longrightarrow p^2 \nmid a_0$

By Eisenstein criterion $f(x) = 8x^3 + 6x^2 - 9x + 24$ *is irreducible over* $\mathbb{Q}$

5. *Show that $f(x) = 2x^5 - 5x^4 + 5$ is irreducible over $\mathbb{Q}$*

Sol: $f(x) = 5 + 0.x + 0.x^2 + 0.x^3 - 5x^4 + 2x^5 \in \mathbb{Z}[x]$

Here $a_0 = 5\,, a_1 = 0, a_2 = 0, a_3 = 0, a_4 = -5, a_5 = 2$

Take $p = 5;\quad 5/5 \Longrightarrow p/a_0; 5/0 \Longrightarrow p/a_1, 5/0 \Longrightarrow p/a_2,$

$5/0 \Longrightarrow p/a_3, 5/-5 \Longrightarrow p/a_4, 5 \nmid 2 \Longrightarrow p \nmid a_5$

$p^2 = 25$ *and* $25 \nmid 5 \Longrightarrow p^2 \nmid a_0$

By Eisenstein criterion $f(x) = 2x^5 - 5x^4 + 5$ *is irreducible over* $\mathbb{Q}$

6. *Show that $f(x) = x^3 - 5x^2 + 10$ is irreducible over $\mathbb{Q}$*

Sol: $f(x) = 10 + 0.x - 5x^2 + x^3 \in \mathbb{Z}[x]$

Here $a_0 = 10\,, a_1 = 0, a_2 = -5, a_3 = 1,$

Take $p = 2$ *or* $5;\quad 5/10 \Longrightarrow p/a_0; 5/0 \Longrightarrow p/a_1, 5/-5 \Longrightarrow p/a_2,$

$5 \nmid 1 \Longrightarrow p \nmid a_5$

$p^2 = 25 \; and \; 25 \nmid 10 \Longrightarrow p^2 \nmid a_0$

By Eisenstein criterion $f(x) = x^3 - 5x^2 + 10$ *is irreducible over* $\mathbb{Q}$

7. *Show that* $f(x) = x^4 - 22x^2 + 1$ ***is irreducible over*** $\mathbb{Q}$

Sol: $f(x) = 1 + 0.x - 22x^2 + 0.x^3 + x^4 \in \mathbb{Z}[x]$

Here $a_0 = 1, a_1 = 0, a_2 = -22, a_3 = 0, a_4 = 1$

Take least prime, $p = 2;\; 2/1 \Longrightarrow p \nmid a_0$

By Eisenstein criterion cannot apply.

$a_0 = 1$ *has two factors* -1 *and* 1 *in* $\mathbb{Z}$

$f(-1) = 1 - 22 + 1 = -20 \neq 0, f(1) = 1 - 22 + 1 = -20 \neq 0$

$\therefore f(x)$ *has no linear factor.*

Now $x^4 - 22x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d)$ *in* $\mathbb{Z}[\boldsymbol{x}]$

$x^4 - 22x^2 + 1 = x^4 + x^3(a + c) + x^2(b + ac + d) + x(ad + bc) + bd$

$\Longrightarrow a + c = 0 \longrightarrow (1), b + d + ac = -22 \longrightarrow (2), ad + bc = 0 \longrightarrow (3), bd = 1 \longrightarrow (4)$

Where $a, b, c, d \in \mathbb{Z}$

From $(4) \Longrightarrow bd = 1 \Longrightarrow b = d = 1$ *or* $b = d = -1$

$b = d = 1$

From $(2) \Longrightarrow 2 + ac = -22 \Longrightarrow ac = -24$

$b = d = -1$

From $(2) \Longrightarrow -2 + ac = -22 \Longrightarrow ac = -20$

From$(1) \Longrightarrow a + c = 0 \Longrightarrow a = -c$

$ac = -24 \;\; and \; a = -c \Longrightarrow c^2 = 24 \; and$

$ac = -20 \; and \; a = -c \Longrightarrow c^2 = 20$

But $c^2 = 24 \;\; or \; c^2 = 20$ *are impossible in* $\mathbb{Z}$

$\therefore \;\; f(x)$ *has no factor of* 2 *nd degree.*

Hence $f(x)$ is irreducible in $\mathbb{Q}$

8. *Prove that $x^2 + x + 4 \in \mathbb{Z}_{11}[x]$ is irreducible over $\mathbb{Z}_{11}$*

Sol: *Let* $f(x) = x^2 + x + 4, \mathbb{Z}_{11} = \{0,1,2,3,4,5,6, \dots 10\} Now f(0) = 4 \neq 0; f(1) = 6 \neq 0;$

$f(2) = 10 \neq 0$

$$f(3) = 9 + 3 + 4 = \frac{16}{11} = 5 \neq 0, f(4) = 16 + 4 + 4 = \frac{24}{11} = 2 \neq 0,$$

$$f(5) = 25 + 5 + 4 = \frac{34}{11} = 1 \neq 0, f(6) = 36 + 6 + 4 = \frac{46}{11} = 2 \neq 0$$

$$f(7) = 49 + 7 + 4 = \frac{60}{11} = 5 \neq 0, f(8) = 64 + 8 + 4 = \frac{76}{11} = 10 \neq 0,$$

$$f(9) = 81 + 9 + 4 = \frac{94}{11} = 6 \neq 0, f(10) = 100 + 10 + 4 = \frac{114}{11} = 4 \neq 0$$

$\therefore x - \alpha$ *where* $\alpha = 0.1,2 \dots 10$ *is not a factor of* $f(x)$.

$\therefore f(x)$ *is irreducible over* $\mathbb{Z}_{11}$

9. *Is $\mathbb{Q}[x]/< x^2 - 5x + 6 >$ is a field? Explain.*

Sol: $f(x) = x^2 - 5x + 6 = (x - 2)(x - 3)$

$\therefore f(x)$*is not irreducible over* $\mathbb{Q}$ *and hence* $< f(x) >$ *is not a maximal ideal of* $\mathbb{Q}[x]$.

Hence $\mathbb{Q}[x]/< f(x) >$ *is not a field*

10. *Is $\mathbb{Q}[x]/< x^2 - 6x + 6 >$ is a field? Explain.*

Sol: $f(x) = x^2 - 6x + 6$ *Here* $a_0 = 6, a_1 = -6, a_2 = 1$

Let $p = 2$, $\quad 2/6 \Longrightarrow p/a_0 . 2/-6 \Longrightarrow p/a_1, 2 \nmid 1 \Longrightarrow p \nmid a_0$

and $p^2 = 4$, $\quad 4 \nmid 1 \Longrightarrow p^2 \nmid a_0$

By Eisenstein criterion $f(x) = x^2 - 6x + 6$ *is irreducible over* $\mathbb{Q}$

$\therefore f(x)$ *is irreducible over* $\mathbb{Q}$ *and hence* $< f(x) >$ *is a maximal ideal of* $\mathbb{Q}[x]$.

Hence $\mathbb{Q}[x]/< f(x) >$ *is a field*

Uniqueness of factorisation theorem: *Let F be a field and $f(x) \in F\{x]$ be a non $-$constant polynomial. Then $f(x)$ can be written as a product of irreducible polynomial in*

$F[x]$ *in a unique way except for order and for unit factor in* F.

Proof: *Let* $f(x) \in F[x]$ *be a non* $-$ *constant polynomial.*

If $f(x)$ *is reducible then* $f(x) = p_1(x)h(x)$ *where* $p_1(x), h(x) \in F[x]$ *with degree of both* $p_1(x), h(x)$ *less than the* $\deg f(x)$.

If both $p_1(x), h(x)$ *are irreducible then proof is over.*

If not, at least one of them, say $h(x)$ *can be written as* $h(x) = p_2(x)v(x)$

where $p_2(x), v(x) \in F[x]$ *with degree of both* $p_2(x), v(x)$ *less than the* $\deg h(x)$.

Proceeding in this way we get $f(x) = p_1(x)p_2(x) \dots p_m(x)$

Where each $p_i(x), i = 1,2,3 \dots m$ *is irreducible.*

If possible suppose that $f(x) = q_1(x)q_2(x) \dots q_n(x)$ *be another factorisation of* $f(x)$.

$\therefore p_1(x)p_2(x) \dots p_m(x) = q_1(x)q_2(x) \dots q_n(x) \rightarrow (1)$

Since $p_1(x)/f(x) \Longrightarrow p_1(x)/q_1(x)q_2(x) \dots q_n(x)$

$\Longrightarrow p_1(x)$ *divides at least one of* $q_1(x), q_2(x), \dots q_n(x)$

Let $p_1(x)/q_1(x)$

Since $q_1(x)$ *is irreducible we have* $q_1(x) = u_1p_1(x)$ *where* $u_1 \neq 0 \in F$ *is a unit.*

From(1); $p_1(x)p_2(x) \dots p_m(x) = u_1p_1(x)q_2(x) \dots q_n(x)$

$\Longrightarrow p_2(x) \dots p_m(x) = u_1q_2(x) \dots q_n(x) \rightarrow (2)$

Repeat, the arguement on the relation (2) *with* $p_2(x)$.

Let $p_2(x)/q_2(x)$

Since $q_2(x)$ *is irreducible we have* $q_2(x) = u_2p_2(x)$ *where* $u_2 \neq 0 \in F$ *is a unit.*

From(2); $p_2(x)p_3(x) \dots p_m(x) = u_1u_2p_2(x)q_3(x) \dots q_n(x)$

$\Longrightarrow p_3(x) \dots p_m(x) = u_1u_2q_3(x) \dots q_n(x) \rightarrow (3)$

If $n > m$ *, after* m *steps we get a relation with* $1 = u_1u_2 \dots u_mq_{m+1}(x) \dots q_n(x)$.

Clearly, the above equation is impossible unless $m = n$

$\therefore$ *We arrive at* $1 = u_1u_2 \dots u_m (\because n = m)$

$Hence\ the\ irreducible\ factors\ p_i(x) and\ q_j(x)\ must\ be\ same\ except\ for\ order\ and\ for\ unit\ factor\ in\ F$