Integral Domain : A non zero commutative ring R without proper zero divisor is called an integral Domain

i.e

$a \cdot b = 0 \Rightarrow$ either $a = 0$ or $b = 0$

Field : A non zero commutative ring with unity '1' is called field if every non zero element is a unit element i.e invertible.

Unit-1

Ring of Polynomial

Def^n : Let R be a ring. By a polynomial over R, we mean an expression of form

$$a_0 + a_1x + a_2x^2 + \ldots\ldots + a_nx^n \qquad a_i \in R$$

Notation $R[x] = \{a_0 + a_1x + a_2x^2 + \ldots + a_nx^n ;\ a_i \in R ;\ n \in Z^+ \cup \{0\}\}$

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

Sol^n T.P $(R[x], +)$ is abelian group

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

$$f(x) = a_0 + a_1x + a_2x^2 + \ldots\ldots + a_nx^n \qquad a_i \in R$$
$$g(x) = b_0 + b_1x + b_2x^2 + \ldots + b_mx^m \qquad b_j \in R$$

Let $n < m$

$$f(x)+g(x) = (a_0+b_0)+(a_1+b_1)x+\dots(a_n+b_n)x^n+b_{n+1}x^{n+1} + \dots\dots + b_m x^m \in R[x]$$

{ as $a_i \in R$ $b_j \in R$; $(R,+)$ is abelian group
$\Rightarrow a_i+b_j \in R$ }

$\Rightarrow f(x)+g(x) \in R[x]$

$\therefore$ Closure holds.

Associative : Let $f(x), g(x), h(x) \in R[x]$

$f(x) = a_0 + a_1x + \dots\dots a_nx^n \quad a_i \in R$
$g(x) = b_0 + b_1x + \dots\dots b_mx^m \quad b_j \in R$
$h(x) = c_0 + c_1x + \dots\dots c_px^p \quad c_k \in R$
$n<m<p$

T.P $f(x)+(g(x)+h(x)) = (f(x)+g(x))+h(x)$

LHS $\Rightarrow f(x)+[(b_0+c_0)+(b_1+c_1)x+\dots(b_m+c_m)x^m + c_{m+1}x^{m+1}+\dots\dots+c_px^p]$

$\Rightarrow [(a_0+(b_0+c_0))+(a_1+(b_1+c_1))x+\dots(a_n+(b_n+c_n))x^n + (b_{n+1}+c_{n+1})x^{n+1}+\dots(b_m+c_m)x^m + c_{m+1}x^{m+1}+\dots \dots + c_px^p]$

{ $\Rightarrow$ as $a_i, b_j, c_k \in R$ R is Ring
$\Rightarrow (a_i+(b_j+c_k)) = ((a_i+b_j)+c_k)$ $\forall\ a_i, b_j, c_k \in R$ }

$\Rightarrow [((a_0+b_0)+c_0)+((a_1+b_1)+c_1)x+\dots+((a_n+b_n)+c_n)x^n + (b_{n+1}+c_{n+1})x^{n+1}+\dots(b_m+c_m)x^m + c_{m+1}x^{m+1}+\dots c_px^p$

$$\Rightarrow \left[\left[(a_0+b_0) + (a_1+b_1)x + \dots (a_n+b_n)x^n \right] + b_{n+1}x^{n+1} + \dots b_m x^m \right] + h(x)$$

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

$$= \text{RHS}$$

Identity: Let $\exists\ g(x) \in R[x]$ s.t

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

$$g(x) = 0$$ i.e polynomial with $a_i = 0\ \forall\ i$

Inverse: Let $\exists\ g(x) \in R[x]$ s.t

$$f(x)+g(x) = 0$$

$$\Rightarrow g(x) = -f(x)$$

$$\Rightarrow g(x) = -a_0 - a_1x - a_2x^2 - \dots - a_nx^n$$

$\{ a_i \in R$ (R is ring $\}$

$\Rightarrow -a_i \in R$

$$\Rightarrow g(x) \in R[x]$$

Abelian: T.P $f(x)+g(x) = g(x)+f(x)$

$$\text{LHS} \Rightarrow f(x)+g(x) = (a_0+b_0) + (a_1+b_1)x + \dots + (a_n+b_n)x^n + b_{n+1}x^{n+1} + \dots + b_m x^m$$

{ as $a_i, b_j \in R$ $\Rightarrow a_i + b_j = b_j + a_i$ — R is Ring $\forall\ a_i, b_j \in R$ }

$\Rightarrow (b_0+a_0) + (b_1+a_1)x + \ldots (b_n+a_n)x^n + b_{n+1}x^{n+1} + \ldots b_m x^m$

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

$= RHS$

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

Distributive :

T.P $(f(x)+g(x)) \cdot h(x) = f(x)\cdot h(x) + g(x)\cdot h(x)$

LHS

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

$= \left((a_0+b_0) + (a_1+b_1)x + \ldots (a_n+b_n)x^n + b_{n+1}x^{n+1} + \ldots b_m x^m\right)\cdot h(x)$

$= (a_0+b_0)c_0 + \left((a_1+b_1)c_0 + (a_0+b_0)c_1\right)x + \ldots \sum_{i+j=k} (a_i+b_i)c_j x^k$

$+ \ldots\ldots + \sum_{i+j=m+p} (a_i+b_i)c_j x^{m+p}$

{ as R is Ring $\therefore (a_i+b_i)\cdot c_j = a_i c_j + b_i c_j$ }

$= (a_0c_0 + b_0c_0) + (a_1c_0 + b_1c_0 + a_0c_1 + b_0c_1)x$

$+ \ldots\ldots \sum_{i+j=k} (a_ic_j + b_ic_j)x^k + \ldots \sum_{i+j=m+p} (a_ic_j + b_ic_j)x^{m+p}$

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

Associative :

T.P $(f(x) \cdot g(x)) \cdot h(x) = f(x) \cdot (g(x) \cdot h(x))$

LHS

$= \left(a_0b_0 + (a_0b_1 + a_1b_0)x + \ldots\ldots + \left(\sum_{i+j=k} a_ib_j\right)x^k + \ldots a_nb_m x^{n+m}\right) \cdot h(x)$

$= (a_0b_0)c_0 + \left((a_0b_1 + a_1b_0)c_0 + (a_0b_0)c_1\right)x + \ldots\ldots$

$\left(\sum_{i+j+l=k} (a_ib_j)c_l\right)x^k + \ldots\ldots (a_nb_m)c_p\, x^{n+m+p}$

{ as R is Ring $\therefore (a_ib_j)c_l = a_i(b_jc_l)$ }

$= a_0(b_0c_0) + \left(a_0(b_1c_0) + a_1(b_0c_0) + a_0(b_0c_1)\right)x + \ldots$

$\ldots + \left(\sum_{i+j+l=k} a_i(b_jc_l)\right)x^k + \ldots\ a_n(b_mc_p)x^{n+m+p}$

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

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

* If identity exist in R, then identity also exist in R[x]
as if $1 \in R$

* If R has multiplicative identity (say) I then multiplicative identity also exist in R[x]

⇒ $a.I = a = I.a \quad \forall a \in R$; let for some $I(x) \in R[x]$ s.t

$f(x).I(x) = f(x) = I(x).f(x) \quad \forall f(x) \in R[x]$

⇒ $I(x) = I + 0x + 0.x^2 + \ldots + 0.x^n$

* If R[x] has multiplicative identity then R also has multiplicative identity.

* If R is commutative, then R[x] is commutative

* If R[x] is commutative, then R is commutative

R[x] is commutative

⇒ $f(x).g(x) = g(x).f(x) \quad \forall f(x), g(x) \in R[x]$

Let $a, b \in R \subseteq R[x]$

⇒ $ab = ba$

∴ R is commutative

Theorem: Let R[x] be ring of polynomials of a ring R and

$f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_mx^m$

$g(x) = b_0 + b_1x + b_2x^2 + \ldots + b_nx^n$

be 2 non zero polynomial of degree m & n respectively then

1. if $f(x)+g(x) \neq 0$, $\deg(f(x)+g(x)) \leq \max(m, n)$
2. If $f(x)g(x) \neq 0$, $\deg(f(x)g(x)) \leq m+n$
3. If R is integral domain then $\deg(f(x).g(x)) = m+n$

4. R is integral domain iff R[x] is integral domain

5. If R is a field, R[x] is never a field.

Proof: ① $f(x)+g(x) = (a_0+b_0)+(a_1+b_1)x+\cdots(a_t+b_t)x^t$

where $t = \max(m,n)$

and $a_k+b_k = 0 \quad \forall \quad k>t$

as $a_k, b_k = 0 \quad \forall \quad k>t$

$$\Rightarrow \deg(f(x)+g(x)) = \begin{cases} t & \text{if } a_t+b_t \neq 0 \\ <t & \text{if } a_t+b_t = 0 \end{cases}$$

Example: $f(x), g(x) \in \mathbb{Z}_6[x]$

$f(x) = 1+2x+3x^2$

$g(x) = 1+3x^2$

$f(x)+g(x) = 2+2x+0x^2$

$= 2+2x$

$\deg(f(x)+g(x)) = 1 < 2$

② $f(x)\cdot g(x) = c_0+c_1x+\cdots c_{m+n}x^{m+n}$

$c_0 = a_0b_0 \qquad c_1 = a_1b_0+a_0b_1$

$c_k = \sum_{i=0}^{k} a_i b_{k-i} \qquad c_{m+n} = a_m b_n$

$$\deg f(x)\cdot g(x) = \begin{cases} m+n & \text{if } c_{m+n} \neq 0 \\ < m+n & \text{if } c_{m+n} = 0 \end{cases}$$

example: $f(x), g(x) \in \mathbb{Z}_6[x]$

$f(x) = 1+2x$

$g(x) = 3x$

$f(x)\cdot g(x) = 3x+6x^2$

$= 3x$ $\quad \deg = 1 < 2$

$f(x) = a_0 + a_1x + \dots a_mx^m \; ; \; a_m \neq 0$

$g(x) = b_0 + b_1x + \dots b_nx^n \; ; \; b_n \neq 0$

(3) $f(x)\cdot g(x) = c_0 + c_1x + \dots + c_{m+n}x^{m+n}$

$c_0 = a_0b_0 \qquad c_1 = a_1b_0 + a_0b_1$

$c_k = \sum_{i=0}^{k} a_i b_{k-i} \qquad c_{m+n} = a_mb_n$

$\deg(f(x)\cdot g(x)) = m+n$ if $c_{m+n} \neq 0$

Here $c_{m+n} \neq 0$

as if $a_m \neq 0 \quad b_n \neq 0$

$\Rightarrow a_mb_n \neq 0$ ($\because$ R is integral domain)

(4) If $R[x]$ is integral domain then as $R \subseteq R[x]$

$\Rightarrow$ R is integral domain

DATE: / / 20
PAGE No

Converse

Let R be integral domain

Let $f(x), g(x) \in R[x] - \{0\}$

$f(x) = a_0 + a_1x + \cdots a_mx^m \quad a_m \neq 0$

$g(x) = b_0 + b_1x + \cdots b_nx^n \quad b_n \neq 0$

$f(x).g(x) = c_0 + c_1x + \cdots + c_{m+n}x^{m+n}$

$c_{m+n} = a_m b_n$

as $a_m, b_n \neq 0$

$\Rightarrow a_m b_n \neq 0$ as R is integral domain

$\Rightarrow c_{m+n} \neq 0$

$\Rightarrow f(x)g(x) \neq 0$

$\therefore R[x]$ is an integral Domain

(5) Let $f(x) = 1+x$

Let there exist $g(x) \in R[x]$ s.t $f(x).g(x) = 1 = g(x).f(x)$

R ⇒ field ⇒ integral domain ∴ R[x] is ID

$\Rightarrow \deg(f(x).g(x)) = \deg(1)$

Field ⇒ Integral Domain ⇒ $\deg(f(x)+g(x)) = \deg f(x) + \deg g(x)$

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

$\Rightarrow \deg g(x) = -\deg f(x)$

$\Rightarrow \deg g(x) = -1$ ⟶ ⟵

$f(x) = 1+x$, $\deg f(x) = 1$

Degree can't be taken -ve in $R[x]$

$\therefore$ inverse does not exist for $f(x) \in R[x]$

Hence $R[x]$ is not a field.

Theorem: for any Commutative ring R

$$\frac{R[x]}{\langle x \rangle} \cong R$$

for $a \in R$

$\langle a \rangle$ = Ideal generated by a

$\langle a \rangle = aR$

$\langle a \rangle = \{ar ; r \in R\}$

Proof: $\theta : R[x] \longrightarrow R$

define $\theta(f(x)) = f(0)$ gives constant term only

Claim: θ is onto homomorphism

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

T.P $\theta(f(x)+g(x)) = \theta(f(x)) + \theta(g(x))$

$\theta(f(x).g(x)) = \theta(f(x)).\theta(g(x))$

Let $f(x) = a_0 + a_1x + \dots a_mx^m$ $\quad n \geq m$

$g(x) = b_0 + b_1x + \dots b_nx^n$

$g(x)$

$$\theta(f(x)+g(x)) = \theta\big((a_0+b_0) + (a_1+b_1)x + \dots + (a_m+b_m)x^m + \dots b_nx^n\big)$$

$$= a_0 + b_0$$

$$= f(0) + g(0)$$

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

$\theta(f(x).g(x)) = \theta(a_0b_0 + (a_0b_1 + a_1b_0)x + \ldots a_mb_n x^{m+n})$

$= a_0b_0$

$= f(0).g(0)$

$= \theta(f(x)).\theta(g(x))$

$\therefore$ Homomorphism exist.

Onto: for any $r \in R$

Take $f(x) = r$

then $\theta(f(x)) = r$

$\therefore$ $R[x] \longrightarrow R$ is onto homomorphism

$\therefore$ by fundamental theorem of homomorphism

$$\frac{R[x]}{\ker\theta} \cong R$$

$\ker\theta = \{ f(x) \in R[x] ;\ \theta(f(x)) = 0 \}$

$= \{ f(x) \in R[x] ;\ f(0) = 0 \}$

i.e polynomials without constant term

$= \{ a_1x + a_2x^2 + \ldots a_nx^n ;\ a_i \in R, n \geq 1 \}$

$= \{ x(a_1 + a_2x + \ldots a_nx^{n-1}) ;\ a_i \in R, n \geq 1 \}$

$= xR[x]$

$= \langle x \rangle$

$\therefore$ $\frac{R[x]}{\langle x \rangle} \cong R$

when $R = \mathbb{Z}$

$$\frac{\mathbb{Z}[x]}{\langle x \rangle} \cong \mathbb{Z}$$

as $\mathbb{Z}$ is integral Domain which is not a field
$\Rightarrow \langle x \rangle$ is prime ideal which is not a maximal ideal.

if $\frac{R}{P}$ is Integral Domain then P is prime ideal

If $\frac{R}{P}$ is field then P is maximal ideal

as field $\Rightarrow$ I.D
$\therefore$ Every maximal ideal is prime ideal

Division algorithm

Let F be a field. for any 2 polynomials $f(x), g(x) \in F[x]$ with $f(x) \neq 0$, $\exists$ unique $q(x), r(x) \in F[x]$ s.t

$f(x) = g(x)q(x) + r(x)$ where
either $r(x) = 0$ or $\deg r(x) < \deg g(x)$

Proof

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

then $f(x) = g(x).\underbrace{0}_{q(x)} + \underbrace{f(x)}_{r(x)}$

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

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

let $f(x) = a_0 + a_1 x + \dots a_m x^m$
$g(x) = b_0 + b_1 x + \dots b_n x^n$

let $f_1(x) = f(x) - a_m b_n^{-1} x^{m-n} g(x)$

$= f(x) - (a_m b_n^{-1} x^{m-n})(b_0 + b_1 x + \dots b_n x^n)$

$= f(x) - (b_0 a_m b_n^{-1} x^{m-n} + \dots + a_m x^m)$

Then degree $f_1(x) < \deg f(x)$

apply PMI

for $n=0$ if $\deg f(x) = 0 = \deg g(x)$

i.e $f(x) = a_0$ & $g(x) = b_0$

we can write $a_0 = (a_0 b_0^{-1}) b_0 + 0$

$\therefore$

$\therefore$ result is true for $n=0$

Let us assume that result is true for all polynomials whose degree is less than degree $f(x)$

$\Rightarrow f_1(x) = q_1(x) g(x) + r_1(x)$

where $r_1(x) = 0$ or $\deg r_1(x) < \deg g(x)$

$\Rightarrow f(x) - (a_m b_n^{-1} x^{m-n}) g(x) = q_1(x) g(x) + r_1(x)$

$\Rightarrow f(x) = (a_m b_n^{-1} x^{m-n}) g(x) + q_1(x) g(x) + r_1(x)$

$= \underbrace{(a_m b_n^{-1} x^{m-n} + q_1(x))}_{q(x)} g(x) + \underbrace{r_1(x)}_{r(x)}$

where $r_1(x) = 0$ or $\deg r_1(x) < \deg g(x)$

$\therefore$ result holds for all $f(x)$

Uniqueness : Let $q(x), q'(x), r(x), r'(x)$ be 2 quotients and remainders respectively, when $f(x)$ is devided by $g(x)$.

$f(x) = g(x)\,q(x) + r(x)$ where $r(x)=0$ or $\deg r(x) < \deg g(x)$

& $f(x) = g(x)\,q'(x) + r'(x)$ where $r'(x)=0$ or $\deg r'(x) < \deg g(x)$

$\Rightarrow g(x)q(x) + r(x) = g(x)q'(x) + r'(x)$

$\Rightarrow g(x)(q(x) - q'(x)) = r'(x) - r(x)$

$\Rightarrow \deg g(x) + \deg(q(x) - q'(x)) = \deg(r'(x) - r(x))$

$\leq \max(\deg r'(x), \deg r(x))$

$< \deg g(x)$

as $\deg r'(x) < \deg g(x)$ and $\deg r(x) < \deg g(x)$

$\Rightarrow$ LHS & RHS are equal only if

$g(x)(q(x) - q'(x)) = r'(x) - r(x) = 0$

$\Rightarrow g(x)(q(x) - q'(x)) = 0$ as $g(x) \neq 0$

$\Rightarrow q(x) - q'(x) = 0$

$\Rightarrow q(x) = q'(x)$

& $r'(x) - r(x) = 0$

$r'(x) = r(x)$

$\therefore \exists$ exist unique $q(x)$ & $r(x)$ s.t

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

Theorem: Every ideal of $\mathbb{Z}$ is a principle ideal

Proof Let $I(\neq 0)$ be an ideal of $\mathbb{Z}$ s.t $I \neq \mathbb{Z}$
Let $a \in I$ be the least non zero element.
Now if $b \in I$ then

$b = aq + r$; $0 \leq r < a$; $q \in \mathbb{Z}$

$r = b - aq \in I$

as by def^n of ideal
$aq \in I$
also $b \in I$
$\Rightarrow b - aq \in I$

$\Rightarrow r = 0$

if $r \neq 0$ then $0 < r < a$; $r \in I$ which contradicts minimality of $a \in I$

$\therefore b = aq$

as $b \in I \Rightarrow aq \in I \Rightarrow I = \langle a \rangle$

$\Rightarrow I = \langle a \rangle \Rightarrow a\mathbb{Z} \subseteq I$ - (1) as $a \in I$
$a \cdot r \in I$
$\Rightarrow$ Also $a\mathbb{Z} \subseteq a\mathbb{Z}$
$\Rightarrow I \subseteq a\mathbb{Z}$
$\Rightarrow I = a\mathbb{Z}$

$\therefore I = \langle a \rangle$ —— is principle ideal

Example of an ideal in a ring which is not a principle ideal

Let $R = \mathbb{Z}[x]$

$I = \langle 2, x \rangle$

$= \{ 2f(x) + x g(x) ; f(x), g(x) \in \mathbb{Z}[x] \}$

Ist we prove I is an ideal

Let $a = 2f(x) + x g(x)$, $b = 2h(x) + x k(x) \in I$

$a - b = 2f(x) + x g(x) + 2h(x) + x k(x)$

$= 2(f(x) - h(x)) + x(g(x) - k(x))$

$= 2R(x) + xS(x) \quad \in I$

r.a $= f(x)\, h(x) \cdot (2f(x) + xg(x))$

$= 2f(x) \cdot h(x) + xg(x) \cdot h(x)$

$= 2P(x) + xQ(x) \quad \in I$

$\therefore$ I is an ideal

Now we will prove result by contradiction

Suppose I is principle ideal

$\Rightarrow I = \langle K(x) \rangle$

for some $K(x) \in \mathbb{Z}[x]$

$I = \langle 2, x \rangle$

$2 \in I \Rightarrow 2 = K(x)\, h(x)$ ——— (*)

for some $h(x), t(x) \in \mathbb{Z}[x]$

$x \in I \Rightarrow x = K(x)\, t(x)$

$\Rightarrow x\, h(x) = K(x)\, t(x)\, h(x)$

$x\, h(x) = 2\, t(x)$ {using (*)}

$\Rightarrow$ each coefficient of $h(x)$ is multiple of 2

$\Rightarrow h(x) = 2(s(x))$ for some $s(x) \in \mathbb{Z}[x]$

put in (*)

$2 = 2K(x) \cdot s(x)$

$\Rightarrow K(x) \cdot s(x) = 1$

$\Rightarrow 1 \in \langle K(x) \rangle$

$\Rightarrow 1 \in I$

$\longrightarrow \quad \longleftarrow$

as $1 \neq 2f(x) + xg(x)$ for any $f(x), g(x) \in \mathbb{Z}[x]$

$\therefore$ I is not principle ideal

Principle ideal Domain

A commutative integral domain with unity is called principle ideal domain (PID) if its every ideal is a principle ideal

eg: $\mathbb{Z}$

Theorem: If f is a field, f[x] is a principle ideal Domain

Let $I(\neq 0)$ be an ideal of f[x]

Let $f(x) \in I$ be a polynomial of least degree and Let $g(x) \in I$

Apply division Algorithm on $f(x), g(x)$

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

$\therefore$ either $r(x) = 0$ or $\deg r(x) < \deg f(x)$

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

$\Rightarrow r(x) = 0$

otherwise $\deg r(x) < \deg f(x)$
leads to contradiction to minimality of $\deg f(x)$

$\Rightarrow g(x) = f(x)q(x)$

$g(x) \in \langle f(x) \rangle$

$\Rightarrow I = \langle f(x) \rangle$

$\therefore I$ is a principle ideal

---

field $\Rightarrow$ Principle ideal domain
$\not\Leftarrow$ (as $\mathbb{Z}$ is PID but $\mathbb{Z}$ is not field)

eg $\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}_p$ eg $\mathbb{Z}, \mathbb{R}[x], \mathbb{Q}[x], \mathbb{C}[x], \mathbb{Z}_p[x]$

Ideals of field F

Let F be any field & $I(\neq 0)$ ideal of F

$\Rightarrow \exists\ a(\neq 0) \in I$ also $a \in F$

$\Rightarrow a^{-1} \in F$

{ as $ra \in I$ for $r \in R$ & $a \in I$ }

$\Rightarrow aa^{-1} \in I$

$\Rightarrow 1 \in I$

$\therefore I = F$

Theorem If unity belongs to ideal then $I = R$ (Ring / field)

(Hint of proof) $\Rightarrow$ for all $r \in F$, $r \cdot 1 \in I$

i.e. $F \subseteq I$

also we know $I \subseteq F$

$\Rightarrow I = F$

$\Rightarrow I = F = \langle 1, \rangle$

∴ Ideals of F are only $\{0\}$ or F

Irreducible polynomial

Let R be a ring and R[x] be ring of polynomials over R. A polynomial $f(x) \in R[x]$ is called irreducible if whenever $f(x) = g(x)\,h(x)$ for some $g(x), h(x) \in R[x]$ then either $g(x)$ or $h(x)$ is unit in R[x].

eg 1. Take $R = \mathbb{Z}[x]$

$f(x) = 2 + 4x$

$= 2(1+2x)$

$g(x)$ is unit, $h(x)$ is not unit

Here none $g(x), h(x)$ is a unit in $\mathbb{Z}[x]$

∴ $f(x)$ is reducible.

2. $R = \mathbb{Q}[x]$

$f(x) = 2 + 4x$

$= 2(1+2x)$

$g(x)$ is unit, $h(x)$ is not unit

Here $g(x) = 2$ is unit in $\mathbb{Q}[x]$. 2 is unit of $\frac{1}{2}$

∴ $f(x)$ is irreducible

DATE / / 20
PAGE NO

Defⁿ for fields

Let F be a field and F[x] be ring of polynomials over F. A polynomial $f(x) \in F[x]$ is called irreducible if whenever $f(x) = h(x)g(x)$ for some $g(x), h(x) \in F[x]$ then either

$g(x) = U(F[x])$ i.e $g(x) \in F \setminus \{0\}$

or

$h(x) = U(F[x])$ i.e $h(x) \in F \setminus \{0\}$

Units of F[x] i.e U(F[x]), F is field

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

$\Rightarrow \exists\ g(x) \in F[x]$ s.t

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

$\Rightarrow \deg(f(x) \cdot g(x)) = \deg(1)$

field $\Rightarrow$ Integral domain $\therefore \deg(f(x) \cdot g(x)) = \deg f(x) + \deg g(x)$

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

$\Rightarrow \deg f(x) = 0 = \deg g(x)$

$\therefore f(x) = a \neq 0 \quad a \in F$

which is clearly invertible as we can take $g(x) = a^{-1}$

eg Take $\mathbb{Z}_2[x]$

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

in $\mathbb{Z}_2$ $\quad 1 \equiv -1$

$\therefore f(x) = 1-x^2$

$= (1-x)(1+x)$

$a \equiv b \pmod n$ if $n \mid a-n$

$2 \mid -1$ i.e $2 \mid 1-2$

$\frac{2}{1}$ i.e $2 \mid -1$

as none $(1-x)$ & $(1+x)$ is unit in $\mathbb{Z}_2[x]$

$\therefore f(x)$ is reducible

eg Take $\mathbb{Z}[x]$

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

$= 1 \cdot (1+x^2)$

as 1 is unit in $\mathbb{Z}[x]$

$\therefore f(x)$ is irreducible

Primitive Polynomial : Let R be a principle ideal Domain. A polynomial $f(x) \in R[x]$ is called primitive polynomial if the gcd of coefficients of $f(x)$ is a unit in R.

eg $2+4x \in \mathbb{Q}[x]$ is primitive as $\gcd(2,4) = 2$ & 2 is unit in $\mathbb{Q}$

Proposition : Let $f(x) \in F[x]$ be a polynomial of degree >1 If $f(\alpha) = 0$ for some $\alpha \in F$, then $f(x)$ is reducible over F.

Given $\deg f(x) > 1$

Proof Let $f(\alpha) = 0$ for some $\alpha \in F$
then apply division algorithm on $f(x)$ & $(x-\alpha)$

$$f(x) = (x-\alpha)\,q(x) + r(x)$$
where either $r(x) = 0$ or $\deg r(x) < 0$

$\Rightarrow f(\alpha) = r(\alpha)$

$\Rightarrow 0 = r(\alpha) = r(x)$ { as $r(x)$ is independent of x $\therefore r(x) = r(\alpha)$ } ↓ using

$\Rightarrow f(x) = (x-\alpha)\,q(x)$

and clearly $\deg q(x) = \deg f(x) - 1 > 0$
as none $(x-\alpha)$ & $q(x)$ is unit in $F[x]$
Hence $f(x)$ is reducible

Proposition: Let $f(x) \in F[x]$ be a polynomial of degree 2 or 3 then $f(x)$ is reducible iff $f(x)$ has a root in F

— deg > 2, 3

Let $x^4 + 5x^2 + 6 \in \mathbb{Q}[x]$
$= (x^2+2)(x^2+3)$ roots are $\pm\sqrt{2}i, \pm\sqrt{3}i \notin \mathbb{Q}$
$\therefore$ no roots but is reducible (as we are able to break it into factors

Proof If $f(x) \in F[x]$ has a root in F
has same proof as above proposition

Converse

Let $\deg(f(x)) = 2$ or 3 and $f(x)$ be reducible

$\Rightarrow f(x) = f_1(x) f_2(x)$ where $f_1(x), f_2(x) \in F[x]$ and $f_1(x), f_2(x) \notin F$

$\Rightarrow \deg(f(x)) = \deg f_1(x) + \deg(f_2(x))$

$\Rightarrow$ at least one of polynomials $f_1(x)$ and $f_2(x)$ has degree 1

(say) $f_1(x)$ has degree 1

$\Rightarrow f_1(x) = ax+b \; ; \; a, b \in F \; ; \; a \neq 0$

$\Rightarrow ax+b \in F[x]$

$\Rightarrow$ Taking $x = -a^{-1}b$

we get $f_1(-a^{-1}b) = a(-a^{-1}b)+b$

$= 0$

$\Rightarrow -a^{-1}b$ is a root of $f_1(x)$

$\Rightarrow -a^{-1}b$ is also a root of $f(x)$

Def^n : Let $a_0 + a_1x + a_2x^2 + \dots a_nx^n \in \mathbb{Z}[x]$ then $\gcd(a_0, a_1, a_2 \dots a_n)$ is called content of the polynomial $f(x)$. we denote it by $c(f)$.

eg: $2+4x \in \mathbb{Z}[x]$

$c(f) = 2 = \gcd(2,4)$

* If content of polynomial is 1 then polynomial is called primitive polynomial.

Lemma : Let $f(x), g(x) \in \mathbb{Z}[x]$. Then $c(fg) = c(f) \cdot c(g)$.
In particular, product of 2 primitive polynomials is primitive.

Proof : Let $c(f) = c$ & $c(g) = d$

$\Rightarrow f(x) = c f_1(x)$ and $g(x) = d g_1(x)$

where $f_1(x)$ and $g_1(x)$ are primitive polynomials over $\mathbb{Z}$

$$\begin{cases} f(x) = 2x^2 + 11x + 8 \\ \quad = 2(1 \cdot x^2 + 5x + 4) \\ \qquad\qquad \text{primitive polynomial} \\ \qquad \text{as } \gcd(1,2,4) = 1 \end{cases}$$

$\Rightarrow fg = cd(f_1 \cdot g_1)$

Taking content on both sides

$$c(fg) = cd\, c(f_1 \cdot g_1)$$

$$= c(f)\, c(g)\, c(f_1 \cdot g_1)$$

Claim $f_1 g_1$ is a primitive polynomials

Assume $f_1 g_1$ is not primitive

$\Rightarrow \exists$ some prime p s.t p devides each coefficients of $f_1 g_1$

assume $f_1(x) = a_0 + a_1 x + \dots a_n x^n$

$g_1(x) = b_0 + b_1 x + \dots b_m x^m$

as f_1, g_1 are primitive polynomials $\Rightarrow \exists$ some a_i s.t $p \nmid a_i$

Let a_r be the first coefficient of $f_1(x)$ which is not divisible by p.

and b_s be the first coefficient of $g_1(x)$ which is not divisible by p.

i.e $p \mid a_i \quad \forall \quad i < r$ but $p \nmid a_r$

$p \mid b_j \quad \forall \quad j < s$ but $p \nmid b_s$

Coefficient of x^{r+s} in $f_1(x)\, g_1(x)$ is

$= a_0 b_{r+s} + a_1 b_{r+s-1} + \dots a_r b_s + a_{r+1} b_{s-1} + \dots a_{r+s} b_0$

$= \Delta$ (say)

as $p \mid a_i \quad i < r$

$\Rightarrow p \mid a_0 b_{r+s}, \; p \mid a_1 b_{r+s-1} \dots, p \mid a_{r-1} b_{s+1}$

as $p \mid b_j \quad j < s$

$\Rightarrow p \mid a_{r+1} b_{s-1}, \; p \mid a_{r+2} b_{s-2} \dots p \mid a_{r+s} b_0$

adding all these terms

$\Rightarrow p \mid (a_0 b_{r+s} + a_1 b_{s+r-1} + \dots + a_{r-1} b_{s+1} + a_{r+1} b_{s-1} + \dots + a_{r+s} b_0)$

$\dots = \lambda$ (say)

$\Rightarrow p \mid \lambda$

as at start we said p devides all coeff of fg.

$\therefore p$ also devides coeff of x^{s+t} $\{$ if $p|a$ & $p|b$ $p|ar+bs$ $\}$

$\Rightarrow p|\Delta$ and $p|\lambda$

$\Rightarrow p|\Delta-\lambda \Rightarrow p|arbs$

$\Rightarrow p|ar$ or $p|bs$

$\longrightarrow$ $\longleftarrow$

as $p\nmid a_r$ and $p\nmid b_s$

Lemma: Let $f(x) \in \mathbb{Z}[x]$ be primitive. Then $f(x)$ is reducible over $\mathbb{Q}$ iff $f(x)$ is reducible over $\mathbb{Z}$

Proof: firstly assume that $f(x) \in \mathbb{Z}[x]$ is reducible over $\mathbb{Z}$

$\Rightarrow f(x) = g(x) \cdot h(x)$ where $g(x), h(x) \in \mathbb{Z}[x]$

as $f(x)$ is primitive $\Rightarrow$ deg $g(x) \geq 1$, deg $h(x) \geq 1$

as $f(x)$ is primitive $\therefore$ we can't write it as $af'(x)$ i.e we can't take anything common except 1

but as we say $f(x)$ is reducible $\therefore$

$f(x) = g(x) \cdot h(x)$ here $g(x)$ or $h(x)$ can't be constants

$\therefore$ deg $g(x) \geq 1$ & deg $h(x) \geq 1$

$\Rightarrow g(x), h(x)$ are non units in $\mathbb{Z}[x]$.

Also $g(x), h(x)$ are non units in $\mathbb{Q}[x]$

$\Rightarrow f(x)$ is reducible in $\mathbb{Q}[x]$

Converse: assume that $f(x) \in \mathbb{Z}[x]$ is reducible over $\mathbb{Q}$

$\Rightarrow f(x) = g(x)\,h(x)$ where $g(x), h(x) \in \mathbb{Q}[x]$

and $g(x), h(x) \notin \mathbb{Q}$ — (*)

$\Rightarrow f(x) = \frac{a}{b}\, g'(x)\, h'(x)$ where $g'(x), h'(x) \in \mathbb{Z}[x]$

also $g'(x)$ & $h'(x)$ are primitive

eg $\left(\frac{1}{2}x^2 + \frac{1}{3}x + 2\right)\left(\frac{2}{4}x^3 + \frac{2}{3}x + 7\right)$

$\Rightarrow \frac{(3x^2+2x^2+2)}{(6)} \cdot \frac{(6x^2+8x+84)}{(12)} = \frac{2}{72}(\quad)(\quad)$

$\Rightarrow b f(x) = a g'(x) h'(x)$ where $g'(x), h'(x) \in \mathbb{Z}[x]$

Taking content on both sides

$b\, c(f(x)) = a\, c(g'(x) \cdot h'(x))$

$b \cdot 1 = a \cdot 1$

$f(x)$ is primitive $\therefore c(f(x)) = 1$

$\Rightarrow b = \pm a$

$\Rightarrow \frac{b}{a} = \pm 1 \qquad \Rightarrow \frac{a}{b} = \pm 1$

put value of $\frac{a}{b}$ in (*)

$f(x) = \pm\, g'(x)\, h'(x)$

where $g'(x), h'(x) \in \mathbb{Z}[x]$

Hence for $f(x)$ is reducible over $\mathbb{Z}$.

Result is not true for irrationals

eg →

$f(x)$ is reducible over $\mathbb{R}\setminus\mathbb{Q}$

$f(x) = x^2 - 3$

$= (x-\sqrt{3})(x+\sqrt{3})$

but $f(x)$ is not reducible over $\mathbb{Z}$

Converse

(x^2-9) is reducible in $\mathbb{Z}$

$(x^2-3)(x^2+3)$

$\notin \mathbb{R}\setminus\mathbb{Q}$

Lemma: If $f(x) \in \mathbb{Z}[x]$ is arbitrary polynomial which is reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$. But the converse may not be true.

Proof Let $f(x) \in \mathbb{Z}[x]$ be arbitrary polynomial which is reducible over $\mathbb{Q}$

$\Rightarrow f(x) = c f_1(x)$ where $c = c(f(x))$ and $f_1(x)$ is primitive

$f_1(x) \in \mathbb{Z}[x]$

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

$\Rightarrow f_1(x)$ is reducible over $\mathbb{Q}$

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

$f(x) = \frac{a}{b} g'(x).h'(x)$

$g(x), h(x) \in \mathbb{Q}[x]$

$g'(x), h'(x) \in \mathbb{Z}[x]$

$g'(x), h'(x)$ are primitive

$\Rightarrow bf(x) = a\, g'(x).h'(x)$

Taking content

$\Rightarrow b\, c(f(x)) = a\, c(g'(x).h'(x))$

$\Rightarrow bc = \pm a \quad \Rightarrow \quad \frac{a}{b} = \pm c$