Eisenstein Irreducibility Criterion

Let $f(x) = a_0 + a_1 x + \dots a_n x^n \in \mathbb{Z}[x]$ where $n \geq 1$ If there exist a prime p s.t $p \mid a_0, p \mid a_1, \dots p \mid a_{n-1}$ but $p \nmid a_n$ and $p^2 \nmid a_0$, then $f(x)$ is irreducible over $\mathbb{Q}$.

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

$\Rightarrow$ $f(x)$ is reducible over $\mathbb{Z}$ also

{using theorem done before}

$\Rightarrow f(x) = g(x) \cdot h(x)$; $g(x), h(x) \in \mathbb{Z}[x]$ & $\deg g(x) \geq 1$ & $\deg h(x) \geq 1$

Let $g(x) = b_0 + b_1 x + \dots b_r x^r$

$h(x) = c_0 + c_1 x + \dots c_s x^s$

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

$\Rightarrow a_0 = b_0 c_0$; $a_n = b_r c_s$ and $n = r+s$

now $p \mid a_0 \Rightarrow p \mid b_0 c_0$

$\Rightarrow$ either $p \mid b_0$ or $p \mid c_0$

and $p^2 \nmid a_0 \Rightarrow p^2 \nmid b_0 c_0 \Rightarrow p$ cannot devide both b_0 and c_0

Hence either $p \mid b_0$ but $p \nmid c_0$ OR $p \nmid b_0$ but $p \mid c_0$

Also $p \nmid a_n \Rightarrow p \nmid b_r c_s \Rightarrow p \nmid b_r$ and $p \nmid c_s$

Case-1 If $p \mid c_0$ but $p \nmid b_0$

as $p \nmid c_s$

Let c_m be the first coefficient of $h(x)$ s.t $p \nmid c_m$

Also we know as $f(x) = g(x) \cdot h(x)$

$\therefore a_m = b_0 c_m + b_1 c_{m-1} + b_2 c_{m-2} \cdots b_m c_0$

$1 \le m \le s$

$\because$ as $s < n = \deg$

$\therefore m < n$

also

$p \mid a_m$ $\quad \{ \because m < n$ (Given in statement)

and $p \mid c_i \quad \forall \quad i < m$

$\Rightarrow p \mid b_1 c_{m-1} + b_2 c_{m-2} + \cdots b_m c_0$

Hence

$p \mid a_m - (b_1 c_{m-1} + b_2 c_{m-2} \cdots b_m c_0)$

$\Rightarrow p \mid b_0 c_m$

$\Rightarrow p \mid b_0$ or $p \mid c_m$

$\rightarrow$ $\leftarrow$

as $p \nmid b_0$ also $p \nmid c_m$

Case 2 If $p \mid b_0$ but $p \nmid c_0$
as $p \nmid b_r$

Let b_t be the first coefficient of $g(x)$ s.t $p \nmid b_t$

Also we know $f(x) = g(x) \cdot h(x)$

$\therefore \quad a_t = b_0 c_t + b_1 c_{t-1} + \cdots b_t c_0$

{ as t can vary in b/w $1 \le t \le r$
as $r < n = r+s$
$\Rightarrow t < n$ }

also
$p \mid a_t \quad \{ \because t < n \}$
and
$p \mid b_i \quad \forall \quad i < t$

$\Rightarrow p \mid b_0 c_t + b_1 c_{t-1} + \cdots b_{t-1} c_1$

$\Rightarrow p \mid a_t - (b_0 c_t + b_1 c_{t-1} + \cdots b_{t-1} c_1)$

$\Rightarrow p \mid b_t c_0$

$\Rightarrow p \mid b_t$ or $p \mid c_0$

$\longrightarrow \quad \longleftarrow$

as $p \nmid b_t$ also $p \nmid c_0$

Hence our assumption was wrong

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

Exercise: $f(x) = 1+x+x^2+x^3+x^4 \in \mathbb{Z}[x]$
check whether $f(x)$ is reducible over $\mathbb{Q}$?

Method 1

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

$1+3$ ✓ root exist

$2+2$

$3+1$ ✓ root exist

root | constant term $\Rightarrow$ root | 1

$\Rightarrow$ root $= \pm 1$

$\longrightarrow$ $\longleftarrow$

then $2+2$

$(a_0+a_1x+a_2x^2)(b_0+b_1x+b_2x^2)$

~~try to break~~

Method-2

$$f(x) = \frac{1-x^5}{1-x}$$

$$f(x+1) = \frac{1-(x+1)^5}{1-(x+1)}$$

$$= \frac{1-[x^5+5x^4+10x^3+10x^2+5x+1]}{-x}$$

$$= \frac{-x[x^4+5x^3+10x^2+10x+5]}{-x}$$

$p = 5$ $\quad p \mid a_1, a_2, a_3, a_4$ but not $p \nmid a_0$

$\therefore f(x+1)$ is irreducible

$\Rightarrow f(x)$ is irreducible

for powers upto $p-1$

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

Ex Let $x^3+ax^2+bx+1 \in \mathbb{Z}[x]$. Prove that $f(x)$ is reducible over $\mathbb{Q}$ iff either $a=b$ or $a+b=-2$

Ex Let $f(x) = x^4+8 \in \mathbb{Z}[x]$. Prove that $f(x)$ is irreducible over $\mathbb{Q}$

Ex Show that $x^3+3x+2 \in \mathbb{Z}_7[x]$ is irreducible over $\mathbb{Z}_7$

Unit-2

Prime element

Def: A non-zero element p of an integral domain R is called a prime element if

1. p is not a unit
2. $p \mid ab$ then $p \mid a$ or $p \mid b$

ex $\mathbb{Z}$ all prime number in $\mathbb{Z}$ are prime element.

$\mathbb{Z}_p$ – p is prime is a field
→ each (+) element in $\mathbb{Z}_p$ is unit
Hence no prime element exist in $\mathbb{Z}_p$ – p prime
Hence no prime element exist in field.

$\mathbb{Q}$ – field, Hence no prime element in $\mathbb{Q}$

$\mathbb{Z}_{10}$ – is not integral domain, ∴ we can't check for prime element.

$\mathbb{R}$ – field, no prime element in $\mathbb{R}$

Irreducible element

Def: A non-zero element p of an integral domain R is called an irreducible element if

1. p is not a unit
2. If $p = ab$ for some $a, b \in R$ then either a is unit or b is unit.

eg In $\mathbb{Z}$ each prime no. is irreducible

Theorem: Let R be an integral domain then every prime element of R is irreducible. But the converse may not be true.

Proof: Let p be a prime element of R.

$\Rightarrow p$ is non zero, non unit also

Let $p = bc$ for some $b, c \in R$ — (1)

T.P $b \in U(R)$ or $c \in U(R)$

now $p = bc \Rightarrow p \mid bc$

as p is prime

$\Rightarrow p \mid b$ or $p \mid c$

Case-I: If $p \mid b$

$\Rightarrow b = pk$ for some $k \in R$

put in (1)

$\Rightarrow p = pkc$

$\Rightarrow p - pkc = 0$

$\Rightarrow p(1-kc) = 0$

$\Rightarrow (1-kc) = 0$ { as p is prime $\therefore p \neq 0$ }

$\Rightarrow$ $kc = 1$ $\Rightarrow$ c is unit element

$\Rightarrow$ $c \in U(R)$

Case-2 If $p \mid c$

$\Rightarrow$ $c = pt$ for some $t \in R$

put in (1)

$\Rightarrow$ $p = bpt$

$\Rightarrow$ $p(1 - bt) = 0$ $\left\{ \begin{array}{l} p \text{ is prime} \\ \therefore p \neq 0 \end{array} \right\}$

$\Rightarrow$ $1 - bt = 0$

$\Rightarrow$ $bt = 1$

$\Rightarrow$ $b \in U(R)$ $\Rightarrow$ b is unit element of R.

Converse is not always true

i.e Example of an Irreducible element in an I.D which is not prime

Let $R = \mathbb{Z}[\sqrt{-5}]$

$= \{ a + b\sqrt{-5} \; ; a, b \in \mathbb{Z} \}$

Claim R is Integral Domain

Let $a + b\sqrt{-5}$, $c + d\sqrt{-5} \in R$.

s.t $(a+b\sqrt{-5})(c+d\sqrt{-5}) = 0$ ——— (1)

Taking conjugate

$(a-b\sqrt{-5})(c-d\sqrt{-5}) = 0$ ——— (2)

(1) × (2) $\in \mathbb{Z}$ as $a, b, c, d, 5$ all are in $\mathbb{Z}$

$\Rightarrow (a^2+5b^2)(c^2+5d^2) = 0$

$\Rightarrow$ either $a^2+5b^2 = 0$ or $c^2+5d^2 = 0$

$\Rightarrow$ either $a=b=0$ or $c=d=0$

$\Rightarrow$ either $(a+b\sqrt{-5}) = 0$ or $(c+d\sqrt{-5}) = 0$

$\therefore$ R is an integral Domain

Now we will find $U(\mathbb{Z}[\sqrt{-5}])$ i.e units of $\mathbb{Z}[\sqrt{-5}]$

Let $a+b\sqrt{-5} \in U(R) \Rightarrow \exists\ c+d\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ s.t

$(a+b\sqrt{-5})(c+d\sqrt{-5}) = 1$ ——— (1)

Taking conjugate

$\Rightarrow$

$(a-b\sqrt{-5})(c-d\sqrt{-5}) = 1$ ——— (2)

(1) × (2)

$\Rightarrow (a^2+5b^2)(c^2+5d^2) = 1$

$\Rightarrow (a^2+5b^2) = \pm 1$ & $(c^2+5d^2) = \pm 1$ & as $a^2, b^2, c^2, d^2 > 0$ $\therefore$ we drop -1

$\Rightarrow a^2+5b^2 = 1$ & $c^2+5d^2 = 1$

if $b \neq 0 \Rightarrow b^2 \geq 1 \Rightarrow 5b^2 \geq 5 \Rightarrow a^2+5b^2 \geq 5$ ⟶ ⟵

$\Rightarrow b = 0$

$\Rightarrow a^2 = 1$

$\Rightarrow a = \pm 1$

similarly $c = \pm 1$

$\therefore$ Units of $\mathbb{Z}[\sqrt{-5}] = \{\pm 1\}$

$U(\mathbb{Z}[\sqrt{-5}]) = \{\pm 1\}$

Consider $3 \in \mathbb{Z}[\sqrt{-5}]$

Claim 3 is irreducible in $\mathbb{Z}[\sqrt{-5}]$

~~On contrary let 3 is reducible~~

$\Rightarrow 3 = \underbrace{(a+b\sqrt{-5})}_{f(x)} \underbrace{(c+d\sqrt{-5})}_{g(x)}$ ——— (1)

T.P either $f(x)$ or $g(x)$ is unit of R

Taking conjugate

$\Rightarrow 3 = (a-b\sqrt{-5})(c-d\sqrt{-5})$ ——— (2)

(1) × (2)

$\Rightarrow 9 = (a^2+5b^2)(c^2+5d^2)$

$\Rightarrow a^2+5b^2 = 1 \; ; \; c^2+5d^2 = 9$

or

$a^2+5b^2 = 3 \; ; \; c^2+5d^2 = 3$

or

$a^2+5b^2 = 9 \; ; \; c^2+5d^2 = 1$

Case-1 If $a^2+5b^2=1$; $c^2+5d^2=9$

$a^2+5b^2=1$

$\Rightarrow b=0$

$\Rightarrow a^2=1 \quad \Rightarrow a=\pm 1$

$\Rightarrow a^2+b\sqrt{-5}=\pm 1$ i.e unit

Case-2 If $a^2+5b^2=3$; $c^2+5d^2=3$

$a^2+5b^2=3$

$\Rightarrow b=0$

$\Rightarrow a^2=3$ not possible

$b\neq 0 \Rightarrow b^2\geq 1$

$\Rightarrow 5b^2\geq 5$

$\Rightarrow a^2+5b^2\geq 5$

as $a\in\mathbb{Z}$

Hence case-2 is not possible.

Case-3 If $a^2+5b^2=9$; $c^2+5d^2=1$

$\Rightarrow c^2+5d^2=1$

$\therefore d=0$

$\Rightarrow c^2=1$

$\Rightarrow c=\pm 1$

$\Rightarrow c+d\sqrt{-5}=\pm 1$ i.e unit

$\therefore$ when $3=(a+b\sqrt{-5})(c+d\sqrt{-5})$

then one of $a+b\sqrt{-5}$ or $c+d\sqrt{-5}$ are units

$\therefore$ 3 is irreducible

Claim 3 is not prime in $\mathbb{Z}[\sqrt{-5}]$

i.e $\exists\ a, b \in \mathbb{Z}[\sqrt{-5}]$ s.t $3 \mid ab$ but $3 \nmid a$ & $3 \nmid b$

clearly $3 \mid 9$

$$9 = (2+\sqrt{5})(2-\sqrt{-5})$$

$$\Rightarrow 3 \mid (2+\sqrt{-5})(2-\sqrt{-5})$$

Let $3 \mid (2+\sqrt{-5})$

we can write if $b \mid a$ then $a = br$ $r \in$ Ring

$$\Rightarrow (2+\sqrt{-5}) = 3(x+y\sqrt{-5})$$

$$\Rightarrow 2 = 3x \quad \& \quad 1 = 3y$$

$$x = \frac{2}{3} \quad \& \quad y = \frac{1}{3}$$

but here $x, y \notin \mathbb{Z}$

$\therefore 3 \nmid (2+\sqrt{-5})$

Similarly $3 \nmid (2-\sqrt{-5})$

$\therefore$ 3 is not prime..

Theorem: In a PID, an element is irreducible iff it is prime

Proof: Let R be a PID and p be a prime element of R

as R is an integral domain $\Rightarrow$ p is irreducible
{using theorem: Let R be an integral domain then every prime element of R is irreducible}

(write proof in exam)

Converse: Let $p \in R$ be irreducible
$\Rightarrow$ p is non zero, non unit
Now let $a, b \in R$ s.t $p \mid ab$

Suppose $p \nmid a$
Consider $I = pR + aR$ { $pR = \{pr ; r \in R\}$
then I is an ideal of R

{Sum of 2 ideals is also an ideal}

but as R is PID $\Rightarrow$ I is principle ideal
$\Rightarrow$ $\exists$ some $c \in R$ s.t

$$I = cR$$

$$\Rightarrow pR + aR = cR \quad \text{---------- (1)}$$

as $p.1 + a.0 = p \in pR + aR$

$$\Rightarrow p \in cR \quad \text{---------- (2)}$$

$\Rightarrow \beta = c.d$ for some $d \in R$

but as β is irreducible so either c or d is a unit

Case 1 if c is a unit

$\Rightarrow c^{-1}$ exist in R.
$\Rightarrow cc^{-1} \in cR$
$\Rightarrow 1 \in cR$ { if unity $\in$ Ideal then Ideal = Ring }
$\rightarrow cR = R$

So from (1)

$$\beta R + aR = R$$

$\Rightarrow 1 \in \beta R + aR$
$\Rightarrow 1 = \beta x + ay$ for some $x, y \in R$
$\Rightarrow b = \beta bx + aby$

Now $\beta \mid \beta$ & $\beta \mid ab$
$\Rightarrow \beta \mid \beta bx + aby$
$\Rightarrow \beta \mid b$

Case-2 If d is unit

d^{-1} exist in R

$\beta = cd$

$\Rightarrow \beta d^{-1} = c$

$\Rightarrow c \in \beta R$

$\Rightarrow \boxed{cR \subseteq \beta R}$

from (2) $\beta \in cR$,

$\Rightarrow \boxed{\beta R \subseteq cR}$

Hence $\beta R = cR$

from (1)

$\beta R + aR = \beta R$

$\beta \cdot 0 + a \cdot 1 \in \beta R$

$\Rightarrow a \in \beta R$

$\Rightarrow a = \beta k$ for some $k \in R$

$\Rightarrow \beta | a$

$\longrightarrow \quad \longleftarrow$ $\therefore$ d can't be unit.

if $a \in bR$ then $aR \subseteq bR$

$a \in bR$

$a = bs$ for some $s \in R$

let $x \in aR$

$x = ar$ for $r \in R$

$= bsr$

$\in bR$

$\Rightarrow aR \subseteq bR$

Q Prove that $\mathbb{Z}[\sqrt{-5}]$ is not a P.I.D.

Sol^n In PID, an element is irreducible $\Leftrightarrow$ prime element but as we did in before example

$3 \in \mathbb{Z}[\sqrt{-5}]$ is irreducible but is not a prime element of $\mathbb{Z}[\sqrt{-5}]$ $\therefore$ $\mathbb{Z}[\sqrt{-5}]$ is not P.I.D

U.f.D

Def^n Let R be an integral domain with unity. Then R is called a unique factorization domain (UFD). if

(i) Every non zero, non unit element in R can be expressed as a finite product of irreducibles in R.

(ii) if $a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$ are two factorizations of 'a' as a product of irreducible elements then $m = n$ and each $p_i = u q_j$ for some j and some $u \in U(R)$

eg

$R = \mathbb{Z}$

non units, non zero $= R \setminus \{0, 1, -1\}$

$10 = 2 \times 5$

$= -2 \times -5$

if we say $10 = p_i q_j$

then $p_i = 1.2$ or -1.2 as $1, -1 \in U(\mathbb{Z})$

Theorem: If R is an integral domain with unity in which each non-zero, non unit element is a finite product of irreducible and every irreducible element is prime, then R is UFD.

Proof T.P that R is UFD, we just need to show that factorization of any non zero, non unit element of R as a finite product of irreducible is unique upto associates.

Let a be a non zero, non unit element which has following factorization

$$a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$$

if $n=1$

$$p_1 = q_1 q_2 \cdots q_m$$

and as p_1 is irreducible

$\Rightarrow$ either q_1 or $q_2 \cdots q_m$ is a unit

$\Rightarrow$ either q_1 or each q_j ; $j \geq 2$ is a unit

$\longrightarrow \leftarrow$ as all q_i's are irreducible

$\Rightarrow m > 1$ is not possible

$\Rightarrow m = 1 \qquad \Rightarrow n = m$

$\Rightarrow a = p_1 = q_1$

Assume that the result is true for elements which can be written as product of $n-1$ irreducibles

Now let $a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$

but as p_1 is irreducible $\Rightarrow$ p_1 is prime

as $p_1 \mid a \Rightarrow p_1 \mid q_i$ for some i

w.l.o.g $p_1 | q_1$

$\Rightarrow q_1 = u p_1$ for some $u \in R$

but q_1 is irreducible

$\Rightarrow$ either u or p_1 is unit

but as p_1 is not unit

$\Rightarrow u$ is a unit $\Rightarrow u \in U(R)$

$\Rightarrow a = p_1 p_2 \cdots p_n = u p_1 q_2 q_3 \cdots q_m$

$\Rightarrow p_1 p_2 \cdots p_n - u p_1 \cdot q_2 q_3 \cdots q_m = 0$

$\Rightarrow p_1 (p_2 p_3 \cdots p_n - u \cdot q_2 q_3 \cdots q_m) = 0$

but $p_1 \neq 0 \Rightarrow (p_2 p_3 \cdots p_n - u q_2 q_3 \cdots q_m) = 0$

$\Rightarrow p_2 p_3 \cdots p_n = u q_2 q_3 \cdots q_m$

$\Rightarrow p_2 p_3 \cdots p_n = q_2' q_3 \cdots q_m$

by induction

$n-1 = m-1$

$\Rightarrow n = m$

for each $2 \leq i \leq n$

$p_i = u_j q_j$ for some $u_j \in U(R)$ & $2 \leq j \leq m$

also $p_1 = u q_1$

Hence factorization is unique upto associates, and hence R is UFD.

Theorem: In a UFD, an element is prime iff it is irreducible.

Proof: Let R be a UFD
and let $a \in R$ be prime
{ as UFD ⇒ Integral Domain
also need to prove in exam }
⇒ a is irreducible

Converse: Let $a \in R$ be irreducible
⇒ a is non-zero and non unit
Let $a|bc$ for some $b, c \in R$

$bc = ak$ for some $k \in R$

If b is unit ⇒ b^{-1} exist in R

⇒ $b^{-1}bc = b^{-1}ak$
⇒ $c = b^{-1}ak = a(b^{-1}k)$

⇒ $a|c$

If c is unit ⇒ c^{-1} exist in R,
⇒ $bcc^{-1} = akc^{-1}$
⇒ $b = a(kc^{-1})$
⇒ $a|b$

So assume that both b & c are non-units
If k is unit $\Rightarrow k^{-1}$ exist in R

$\Rightarrow bck^{-1} = akk^{-1}$

$\Rightarrow bck^{-1} = a$

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

but a is irreducible

$\Rightarrow$ either $b \in U(R)$ or $ck^{-1} \in U(R)$

but b is non units

$\Rightarrow ck^{-1} \in U(R)$

$\Rightarrow ck^{-1}k \in U(R)$ $\quad [\because k \in U(R)]$

$\Rightarrow c \in U(R)$

$\longrightarrow \quad \longleftarrow$

If b & c are non units, k is also a non unit

so $bc = ak$ ——— (*)

as b, c, k are non-zero, non-units elements of R, which is a UFD

so

$b = p_1 p_2 \dots p_m$

$c = q_1 q_2 \dots q_m$

$k = s_1 s_2 \dots s_t$

where p_i's, q_j's, s_t's are irreducible elements.

so from (*)

$$p_1 p_2 \cdots p_n q_1 q_2 \cdots q_m = a r_1 r_2 \cdots r_t = x \text{ (say)}$$

as R is UFD

$\Rightarrow$ $n+m = 1+t$ & $a = u p_i$ or $a = u q_j$ for some $u \in U(R)$

$\Rightarrow$ $u^{-1}a = p_i$ or $u^{-1}a = q_j$

$\Rightarrow$ $a \mid p_i$ or $a \mid q_j$

$\Rightarrow$ $a \mid p_1 p_2 \cdots p_n$ or $a \mid q_1 q_2 \cdots q_m$

$\Rightarrow$ $a \mid b$ or $a \mid c$

While defining Content we take $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ but not in some general $R[x]$

because in $\mathbb{Z}$, $\gcd(a_0, a_1, \cdots a_n)$ always exist but in any general ring we are not sure gcd exist or not

for ex Take Ring $\mathbb{Z}[\sqrt{-3}]$

Take $4, 2(1+\sqrt{-3}) \in \mathbb{Z}[\sqrt{-3}]$

$$\gcd(4, 2(1+\sqrt{-3})) = 2 \gcd(2, 1+\sqrt{-3}) = 2 \quad \text{---(1)}$$

Also $4 = (1+\sqrt{-3})(1-\sqrt{-3})$

as $1+\sqrt{-3}$ is irreducible

Let $(1+\sqrt{-3}) = (x+iy\sqrt{3})(a+ib\sqrt{3})$

Take conjugate

$(1-\sqrt{-3}) = (x-iy\sqrt{3})(a-ib\sqrt{3})$

$\Rightarrow$ & $4 = (x^2+3y^2)(a^2+3b^2)$

$\Rightarrow$ $x^2+3y^2 = 2 = a^2+3b^2$

or $x^2+3y^2 = 4$ $a^2+3b^2 = 1$ & vice versa

$\Rightarrow$ $\gcd(4, 2(1+\sqrt{-3})) = \gcd((1+\sqrt{-3})(1-\sqrt{-3}), 2(1+\sqrt{-3}))$

$= (1+\sqrt{-3})\gcd(2(1-\sqrt{-3}), 2)$

$= (1+\sqrt{-3})$ ——— (2)

as $\gcd(4, 2(1+\sqrt{-3}))$ is not unique.
from (1) & (2) $\therefore$ gcd doesn't exist of $(4, 2(1+\sqrt{-3}))$ in $\mathbb{Z}[\sqrt{-3}]$.

Theorem: If a UFD, any two non zero elements have g.c.d.

Proof: Let R be a UFD and a, b be any 2 non zero elements in R.

If a is unit
$\Rightarrow a^{-1}$ exist in R
$\therefore \quad b = baa^{-1}$

$\therefore \gcd(a,b) = \gcd(a, baa^{-1})$
$= \gcd(a, aba^{-1})$ {$\because$ R is commutative}
$= a\gcd(1, ba^{-1})$
$= a$

Similarly if b is unit $\gcd(a,b) = b$

If a, b are non units
$\therefore$ as R is UFD

$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$

$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}$ where $\alpha_i \geq 0$ & $\beta_j \geq 0$

{ $30 = 2 \times 3 \times 5$
$50 = 2 \times 5 \times 5 = 2^1 \times 3^0 \times 5^2$ }

Let $r_i = \min\{\alpha_i, \beta_i\}$ $\forall$ $1 \le i \le n$

then

Claim $d = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}$ is gcd of a, b

$d = \gcd(a,b)$ if

① $d \mid a$ and $d \mid b$

② if $c \in R$ s.t $c \mid a$ & $c \mid b$ then $c \mid d$

Now

$a = d\, p_1^{\alpha_1 - r_1} p_2^{\alpha_2 - r_2} \cdots p_n^{\alpha_n - r_n}$

clearly $\alpha_i - r_i \ge 0$

$\Rightarrow d \mid a$

Similarly $d \mid b$

Now let $c \in R$ s.t $c \mid a$ & $c \mid b$

T.P $c \mid d$

If c is unit, then c^{-1} exist in R

$\Rightarrow d = cc^{-1}d$

$\Rightarrow \underline{c \mid d}$

If c is non unit then as $c \mid a$ & $c \mid b$

$\Rightarrow c = p_1^{s_1} p_2^{s_2} \cdots p_n^{s_n}$

as $c \mid a \Rightarrow s_i \le \alpha_i \quad \forall i$

as $c \mid b \Rightarrow s_i \le b_i \quad \forall i$

$\Rightarrow s_i \le \min\{\alpha_i, \beta_i\}$

$\Rightarrow \quad r_i \leq \gamma_i$

$\Rightarrow \quad r_i \leq \gamma_i \qquad \forall \; 1 \leq i \leq n$

$\Rightarrow \quad p_i^{\gamma_i} = p_i^{r_i} \cdot p_i^{\gamma_i - r_i} \qquad \forall \; 1 \leq i \leq n$

$\Rightarrow \quad p_i^{r_i} \mid p_i^{\gamma_i} \qquad \forall \; 1 \leq i \leq n$

$\Rightarrow \quad p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n} \mid p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_n^{\gamma_n}$

$\Rightarrow \quad c \mid d$

Hence d is gcd

Theorem: Every PID is a UFD

Proof: Let R be a PID. Then R is integral domain with unity and each irreducible element of R is prime.

T.P that R is UFD, we just need to proof that each non zero, non unit element of R can be written as finite product of irreducible elements of R

for this we will show that a PID cannot have an infinite ascending chain of ideals

$12\mathbb{Z} \subseteq 6\mathbb{Z} \subseteq 3\mathbb{Z} \subseteq \mathbb{Z}$ —— ascending chain

$3\mathbb{Z} \supseteq 6\mathbb{Z} \supseteq 12\mathbb{Z} \supseteq 24\mathbb{Z} \supseteq 48\mathbb{Z}$ —— descending chain

i.e chain $I_1 \subseteq I_2 \subseteq I_3 \ldots$ of ideals stop after finitely many steps.

as R is P.I.D , $I_k = a_k R$ for some $a_k \in R$

$\Rightarrow$ chain is

$a_1R \subseteq a_2R \subseteq a_3R \subseteq \ldots\ldots$

Consider $\bigcup a_i R = A$

Claim A is ideal of R

clearly $A \neq \phi$ as $a_1R \subseteq A$ & $a_1R \neq \phi$

Let $x, y \in A$

then

$x \in a_iR$ for some i

$y \in a_jR$ for some j

w.l.o.g let $i<j$ & as $a_1R \subseteq a_2R \subseteq \ldots$

$\therefore \Rightarrow a_iR \subseteq a_jR$

$\Rightarrow x \in a_jR$

$\Rightarrow x-y \in a_jR$ ($\because x, y \in a_jR$ & a_jR is ideal)

$\Rightarrow x-y \in A$

Let $x \in A$ and $r \in R$

$x \in a_iR$ for some i

$\Rightarrow xr \in a_iR$ for some i { $\because a_iR$ is ideal }

$\Rightarrow x_1, x \in \cup a_i R$

$\Rightarrow x_1, x \in A$

Hence $A \trianglelefteq R$

$A = \cup a_i R$ is an ideal of R and R is PID

$\Rightarrow A = aR$ for some $a \in R$

$\Rightarrow \cup a_i R = aR$

$\Rightarrow$ <u>each $a_i R \subseteq aR$</u>

Also $a \in aR$ { as $\cup a_i R = aR$ }

$\Rightarrow a \in \cup a_i R$

$\Rightarrow a \in a_k R$ for some k

$\Rightarrow$ <u>$aR \subseteq a_k R$</u> for some k

So $a_k R \subseteq aR \subseteq a_k R$

$\Rightarrow a_k R = aR = \cup a_i R$

$\rightarrow a_k R \subseteq a_{k+i} R \subseteq aR$ for $i \geq 1$

$\rightarrow a_k R = aR = a_{k+i} R$ $\forall\ i \geq 1$

Now let $a \in R$ be a non zero, non unit element

T.P a can be written as a finite product of irreducible elements.

If a is irreducible, then nothing to prove

So assume that a is reducible

$\Rightarrow \quad a = bc \quad ; b, c \in R$ and both b, c are non-units

if both b and c are finite product of irreducibles then a is also finite product of reducibles

So, assume that atleast one of b & c; (say) b is not finite product of irreducibles.

$\Rightarrow \quad b = xy$ where x cannot be written as a finite product of irreducibles

and we can continue this process infinitely many times so that we have

as $a = bc \Rightarrow a \in bR \Rightarrow aR \subseteq bR$

and

$b = xy \Rightarrow b \in xR \Rightarrow bR \subseteq xR$

and so on

i.e $aR \subseteq bR \subseteq xR \subseteq \ldots\ldots$ is an infinite chain of ideals of R, which doesn't terminate but R is a PID, this chain must stop after finitely many step

$\Rightarrow$ Our assumption that b is not a finite product

of irreducible elements is false.

⇒ both b & c are finite product of irreducibles

⇒ a is also a finite product of irreducibles

Converse : May not be true

we need to provide example of a UFD which is not a PID

(1) $\mathbb{Z}[x]$ is non PID but $\mathbb{Z}[x]$ is a UFD

(2) let F - field

$R = F[x]$ —— PID

⇒ R is UFD also

Result Now if R is UFD then $R[y]$ is UFD

⇒ $R[y]$ is UFD

⇒ $F[x][y]$ is UFD

$F[x][y] = F[x,y]$ is UFD

Consider $I = xR + yR$

Claim I is not PI

let $I = \langle f(x,y) \rangle$

as $x \in I \Rightarrow x = g(x,y)f(x,y)$

as $y \in I \Rightarrow y = h(x,y)f(x,y)$

$\Rightarrow x = gf$

$y = hf$

$\Rightarrow \frac{x}{g} - \frac{y}{h} = 0$

$\Rightarrow hx = gy$

as x & y are 2 variables they can't satisfy such relation

∴ I is not principle ideal

Thm: if R is UFD, then R[x] is also UFD

$\mathbb{Z}$ - PID
$\mathbb{Z}[x]$ ≠ PID

F - Field
F[x] ≠ field

DATE: / / 20
PAGE No

Euclidean Domains (ED's)

Def^n: A commutative integral domain R with unity is called Euclidean domain (ED) if ∃ a function

$\phi : R^* \to \mathbb{Z}$ satisfying the following axioms

(i) $a, b \in R^* = R - \{0\}$ and $b \mid a$ then $\phi(b) \leq \phi(a)$

(ii) for each pair of elements $a, b \in R$, $b \neq 0$, ∃ elements $q, r \in R$ s.t $a = bq + r$ where $r = 0$ or $\phi(r) < \phi(b)$

↓ Euclidean algorithm

Example: $R = \mathbb{Z}$

$\phi : \mathbb{Z} \to \mathbb{Z}$

$\phi(a) = |a|$

if we take $\phi(a) = a$ then $b \mid a \not\Rightarrow b < a$ as $2 \mid -2$ but $2 \not< -2$

① $b \mid a$, then $|b| \leq |a| \Rightarrow \phi(b) \leq \phi(a)$

② Let $a, b \in \mathbb{Z}$, $b \neq 0$
then by division algorithm

$a = bq + r$ where $0 \leq r < |b|$
$\Rightarrow 0 \leq |r| < |b|$

$\Rightarrow a = bq + r$ where either $r = 0$ or $\phi(r) < \phi(b)$

Example-2 $F[x]$ where F is field

Define $\phi : F[x] \longrightarrow \mathbb{Z}$

$\phi(f(x)) = \deg(f(x))$

(i) Let $b \in R^*$, $b|a$ then $\phi(b) \leq \phi(a)$

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

s.t $g(x) | f(x)$

$\Rightarrow f(x) = h(x) \cdot g(x)$ for some $h(x) \in F[x]$

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

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

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

$\Rightarrow \phi(f(x)) \geq \phi(g(x))$

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

by division algorithm

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

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

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

$\therefore$ $F[x]$ is Euclidean Domain

Example -3 $\mathbb{Z}[i]$ – Ring of Gaussian integers

$\mathbb{Z}[i] = \{a+bi ;\ a, b \in \mathbb{Z}\}$

* Prove $(\mathbb{Z}[i], +, \times)$ is Ring & Integral Domain

Proof for integral Domain →

$(a+bi)(c+di) = 0$

Taking Conjugate

$(a-bi)(c-di) = 0$

$(a^2+b^2)(c^2+d^2) = 0$

as $a, b, c, d \in \mathbb{Z} \Rightarrow (a^2+b^2) \in \mathbb{Z}$

as $\mathbb{Z}$ is integral Domain

$\Rightarrow a^2+b^2 = 0$ or $c^2+d^2 = 0$

$\Rightarrow a = 0$ & $b = 0$ or $c = 0$ & $d = 0$

Now define $\mathbb{Z}[i] \longrightarrow \mathbb{Z}$

$\phi(a+bi) = a^2+b^2$

Ist

(i) $x, y \in \mathbb{Z}[i]^*$ $y \neq 0$ & $y \mid x$ then $\phi(y) \leq \phi(x)$

Let $x = a+bi$

and $y = m+ni$

as $y|x \Rightarrow x = yz$ for some $z \in \mathbb{Z}[i]$

let $z = c+di$ for some $c, d \in \mathbb{Z}$

$\phi(x) = \phi(a+bi) = a^2+b^2$

Also

$\phi(x) = \phi(yz) = \phi((mc-nd)+i(md+nc))$

$= (mc-nd)^2 + (md+nc)^2$

$= m^2c^2 + n^2d^2 - 2mcnd + m^2d^2 + n^2c^2 + 2mdnc$

$= m^2(c^2+d^2) + n^2(c^2+d^2)$

$= (m^2+n^2)(c^2+d^2)$

$= \phi(y)\,\phi(z) \geq \phi(y)$

$\Rightarrow \phi(x) \geq \phi(y)$

(ii) for $x, y \in \mathbb{Z}[i]$, $y \neq 0$ $\exists$ $q, r \in \mathbb{Z}[i]$ s.t $x = qy + r$ where either $r = 0$ or $\phi(r) < \phi(y)$

let $x = a+bi$

$y = m+ni$

$\frac{x}{y} = \frac{a+bi}{m+ni}$

rationalising

$$\frac{x}{y} = \frac{(a+bi)}{(m+ni)}\frac{(m-ni)}{(m-ni)} = \frac{(am+bn)+i(bm-an)}{m^2+n^2}$$

$$= \alpha + \beta i \quad \text{where } \alpha, \beta \in \mathbb{Q}$$

we can always find integers α_0 & β_0 s.t

$$|\alpha - \alpha_0| \leq \frac{1}{2} \quad \text{and} \quad |\beta - \beta_0| \leq 1/2$$

$$\Rightarrow x = y(\alpha + \beta i)$$

$$x = y(\alpha - \alpha_0 + \alpha_0 + (\beta - \beta_0 + \beta_0)i)$$

$$x = \underbrace{y(\alpha_0 + \beta_0 i)}_{q} + y[(\alpha - \alpha_0) + (\beta - \beta_0)i]$$

Here $y[(\alpha - \alpha_0) + (\beta - \beta_0)i] = x - yq \in \mathbb{Z}[i]$

$\therefore r = y[(\alpha - \alpha_0) + (\beta - \beta_0)i] \in \mathbb{Z}[i]$

$\therefore x = yq + r$ where $q = \alpha_0 + \beta_0 i$

$r = y[(\alpha - \alpha_0) + (\beta - \beta_0)i]$

If $r = 0$; then nothing to prove

If $r \neq 0$

$$\phi(z) = \phi\left(y\left((\alpha-\alpha_0)+(\beta-\beta_0)i\right)\right)$$

$$= y^2\left((\alpha-\alpha_0)^2+(\beta-\beta_0)^2\right)$$

$$\because \{\text{using } \phi(x) = \phi(yz) = \phi(y)\phi(z) \text{ for } x=yz\}$$

$$\phi(z) = \phi(y)\,\phi\left((\alpha-\alpha_0)+(\beta-\beta_0)i\right)$$

$$= \phi(y)\left[(\alpha-\alpha_0)^2+(\beta-\beta_0)^2\right]$$

$$\leq \phi(y)\left[\frac{1}{4}+\frac{1}{4}\right] \quad \left\{\because |\alpha-\alpha_0| \leq 1/2,\ (\alpha-\alpha_0)^2 \leq \frac{1}{4}\right.$$

$$= \phi(y)\left[\frac{1}{2}\right]$$

$$= \frac{\phi(y)}{2}$$

$$< \phi(y)$$

$$\Rightarrow \phi(z) < \phi(y)$$

Theorem: Every ED is a PID

Proof: Let R be a E.D. Then R is commutative integral Domain with unity

T.P R is PID we just need to show that every ideal of

R is a principle ideal.

Let I be a non zero ideal of R

$\Rightarrow \exists$ some $a \in I$ s.t $a \neq 0$
also $1|a \Rightarrow \phi(a) \geq \phi(1)$ { by property of E.D }

Construct $S = \{ \phi(a) ; a \in I \} \subseteq \mathbb{Z}$

{ as $\phi : R \to \mathbb{Z} \Rightarrow \phi(a) \in \mathbb{Z} \ \forall \ a \in I \subseteq R$
$\therefore S \subseteq \mathbb{Z}$ }

and $\phi(1)$ is lower bound of S { as $\phi(a) \geq \phi(1) \ \forall a \in I$ }

$\therefore$ by well ordering principle

S has a least element (say) $\phi(d)$ where $d \in I$

Claim $I = dR$

Let $b \in I$
$b = dq + r$ where either $r = 0$ or $\phi(r) < \phi(d)$
{ using 2nd property of euclidian Domain }

$r = b - dq$ { $b \in I \ d \in I \ q \in R \Rightarrow dq \in I \Rightarrow b - dq \in I$ }

$\Rightarrow r \in I$
$\Rightarrow \phi(r) \geq \phi(d)$ { $\because \phi(d)$ is least element }

Now as $\phi(r) \not< \phi(d) \ \therefore \ r = 0$

$\Rightarrow b = dq$

$\Rightarrow b \in dR$

Hence $I = dR$

$\Rightarrow R$ is a PID

Q: Is every PID, a ED also?

Sol: No,

eg $\mathbb{Z}[\sqrt{-19}]$

$\mathbb{Z}[\sqrt{-19}] = \{ a+b\sqrt{-19} \; ; \; a, b \in \mathbb{Z}$ & a, b are of same parity $\}$

either both even or both odd

Thm: Every field is a ED

Define $\phi : F \longrightarrow \mathbb{Z}$

$$\phi(a) = \begin{cases} 1 \; ; \; a \neq 0 \\ 0 \; ; \; a = 0 \end{cases}$$

Field → E.D → P.I.D → U.F.D

DATE: / / 20
PAGE NO

Lemma: Let f be a primitive polynomial in $\mathbb{Z}[x]$ and let g be any polynomial in $\mathbb{Z}[x]$. Suppose f devides g in $\mathbb{Q}[x]$ say $g = fq$ with $q \in \mathbb{Q}[x]$. Then $q \in \mathbb{Z}[x]$ and hence f devides g in $\mathbb{Z}[x]$.

Proof: we can write $q = \frac{a}{b} q_0$ where $q_0 \in \mathbb{Z}[x]$ is a primitive polynomial

if $q = \frac{2}{3} + \frac{4}{5}x$

$= \frac{10+12x}{15}$

$= \frac{2}{15}(5+6x)$

$= \frac{a}{b} q_0$ $\quad q_0 \in \mathbb{Z}[x]$ also $\gcd(5,6) = 1$

as $g = fq$

$\Rightarrow g = f \cdot \frac{a}{b} q_0$

$\Rightarrow bg = af q_0$

Taking content on both sides

$\Rightarrow b \cdot c(g) = a\, c(f q_0)$

$\Rightarrow b \cdot c(g) = a$ { by Gauss Lema product of 2 primitive is primitive

$\Rightarrow b \mid a$

$\Rightarrow \frac{a}{b}$ is integer.

and $q(x) = \frac{a}{b} q_0(x)$ where $q_0(x) \in \mathbb{Z}'[x]$

$= \text{integer} \times q_0(x)$

$\in \mathbb{Z}'[x]$

Theorem $\mathbb{Z}'[x]$ is a UFD

Proof As $\mathbb{Z}'$ is commutative Integral Domain with unity $\Rightarrow \mathbb{Z}'[x]$ is also commutative integral Domain with unity.

Claim Every Non zero, non unit element of $\mathbb{Z}'[x]$ can be

written as a finite product of irreducibles element of $\mathbb{Z}[x]$

Let $f(x) \in \mathbb{Z}[x]$ be non zero non unit element

We prove it by PMI on $\deg f(x)$

→ If $\deg f(x) = 0 \Rightarrow f(x) = a \in \mathbb{Z}$

as $\mathbb{Z}$ is UFD, 'a' can be written as finite product of irreducible elements of $\mathbb{Z} \subseteq \mathbb{Z}[x]$

→ If $\deg f(x) = 1$

then $f(x) = c f_0(x)$, where $f_0(x) \in \mathbb{Z}[x]$ is primitive which is again a finite product of irreducibles as $c \in \mathbb{Z}$ and $f_0(x) \in \mathbb{Z}[x]$ is irreducible.

→ Now assume that the result is true for polynomials whose degree is less than n

→ Let $\deg f(x) = n$. Also we can assume $f(x)$ is primitive
{∵ otherwise $f(x) = c f_0(x)$ where $c \in \mathbb{Z}$, $f_0(x) \in \mathbb{Z}[x]$ & f is primitive & factorization of $f(x)$ follows from that of $f_0(x)$}
If $f(x)$ is irreducible, then nothing to prove

So assume $f(x)$ is reducible

$\Rightarrow f(x) = f_1(x) f_2(x)$, where $\deg f_1(x) = n_1$, $\deg f_2(x) = n_2$

and $1 \leq n_1 < n$
$1 \leq n_2 < n$

{as $f_1(x)$, $f_2(x)$ can't be units / constants}

by Induction hypothesis

both $f_1(x)$ & $f_2(x)$ can be written as finite product of irreducible elements of $\mathbb{Z}[x]$ and hence $f(x)$ is written as finite product of irreducibles

T.1 Every irreducible element of $\mathbb{Z}[x]$ is a prime element

Let $f(x) \in \mathbb{Z}[x]$ is irreducible element and $f(x) \mid g(x).h(x)$ in $\mathbb{Z}[x]$

Case-1 if $\deg f(x) = 0 \Rightarrow f(x) = a \in \mathbb{Z}$

now $g(x) = c\, g_0(x)$ where $c = c(g(x))$ & $g_0(x) \in \mathbb{Z}[x]$ is primitive polynomial

$h(x) = d\, h_0(x)$ where $d = c(h(x))$ & $h_0(x) \in \mathbb{Z}[x]$ is primitive polynomial

now $f(x) \mid g(x).h(x) \Rightarrow a \mid cd\, g_0(x) h_0(x)$

also $a \nmid g_0(x)$ & $a \nmid h_0(x)$

{ $\because$ a is non unit being irreducible and $g_0(x)$ & $h_0(x)$ are primitive }

$\Rightarrow a \mid cd$ here $a, c, d \in \mathbb{Z}$

$\Rightarrow a \mid c$ or $a \mid d$

{because every irreducible element of $\mathbb{Z}$ is prime}

$\Rightarrow a \mid c g_0(x)$ or $a \mid d h_0(x)$

$\Rightarrow a \mid g(x)$ or $a \mid h(x)$

$\Rightarrow f(x) \mid g(x)$ or $f(x) \mid h(x)$

Case-2 If $\deg f(x) \geq 1$

As $f(x)$ is irreducible
$\Rightarrow f(x)$ is primitive

as $f(x)$ is irreducible & primitive polynomial in $\mathbb{Z}[x]$

$\Rightarrow f(x)$ is irreducible, primitive polynomial in $\mathbb{Q}[x]$

∵ otherwise we can write $f(x) = c f_0(x)$ here $c = c(f(x))$ & $f_0(x)$ is primitive where $\deg f_0(x) = \deg f(x)$ and $c(f) \notin U(\mathbb{Z})$

$f(x) = c(f) f_0(x)$

both monunits

as $f(x)$ is irreducible

$\therefore f(x) \in \mathbb{Q}[x]$ is an irreducible element but $\mathbb{Q}[x]$ is a PID [∵ $F[x]$ is a PID, if F is a field]

$\Rightarrow f(x)$ is a prime element in $\mathbb{Q}[x]$

{∵ in PID, every irreducible element is prime}

so if $f(x) \mid g(x) h(x) \Rightarrow f(x) \mid g(x)$ or $f(x) \mid h(x)$ in $\mathbb{Q}[x]$

$\Rightarrow f(x) \mid g(x)$ or $f(x) \mid h(x)$ in $\mathbb{Z}[x]$

{ by Lemma }

Hence $f(x)$ is a prime element in $\mathbb{Z}[x]$

so $\mathbb{Z}[x]$ is a UFD

Unit-3

Linear transformation : Let V & W be 2 vector spaces over a field f then $T: V \to W$ is called linear transformation if

1. $T(v_1 + v_2) = T(v_1) + T(v_2)$ $\forall\ v_1, v_2 \in V$
2. $T(\alpha v) = \alpha T(v)$ $\forall\ \alpha \in f$ & $v \in V$

(or)

$T(\alpha v_1 + v_2) = \alpha T(v_1) + T(v_2)$ $\forall\ \alpha \in f;\ v_1, v_2 \in V$

* Suppose T_1, T_2 are 2 linear transformations from V to W then $(T_1 + T_2)(x) = T_1(x) + T_2(x)$ is also a linear transformation

Let $\alpha \in f$ & $v_1, v_2 \in V$

$$(T_1 + T_2)(\alpha v_1 + v_2) = T_1(\alpha v_1 + v_2) + T_2(\alpha v_1 + v_2)$$

$$= \alpha T_1(v_1) + T_1(v_2) + \alpha T_2(v_1) + T_2(v_2)$$

$$= \alpha(T_1(v_1) + T_2(v_1)) + T_1(v_2) + T_2(v_2)$$

$$= \alpha(T_1 + T_2)(v_1) + (T_1 + T_2)(v_2)$$

* Let $T_1, T_2, T_3 \in \text{Hom}(V, W)$

$\{T: V \to W,\ T \text{ is linear trans}\} = \text{Hom}(V, W)$

$(T_1+T_2)+T_3 = T_1+(T_2+T_3)$

RTP

$((T_1+T_2)+T_3)(v) = (T_1+T_2)(v) + T_3(v)$

$= T_1(v) + T_2(v) + T_3(v)$

$= T_1(v) + (T_2+T_3)(v)$

$= (T_1+(T_2+T_3))(v)$

* Does $\exists$ any L.T $T': V \to W$ s.t

$T+T' = T = T'+T \quad \forall\ T \in Hom(V,W)$

T.P $(T+T')(v) = T(v) \quad \forall\ v \in V$

$T(v) + T'(v) = T(v)$

$T'(v) = 0 \quad \forall\ v \in V$

$\Rightarrow T': V \to W$ is defined by

$T'(v) = 0$

which is a linear transformation

$\Rightarrow$ ~~T'(v)~~ T' is identity of $Hom(V,W)$ under addition.

V

Let $T \in \text{Hom}(V,W)$

Then $-T(\alpha v_1 + v_2) = -(\alpha T(v_1) + T(v_2))$

$= -\alpha T(v_1) - T(v_2)$

$= \alpha(-T)(v_1) + (-T)(v_2)$

$\Rightarrow -T \in \text{Hom}(V,W)$

and $T(v) + (-T)(v) = T(v) - T(v) = 0 \quad \forall v \in V$

$\therefore$ $-T$ is inverse of T

Let $T_1, T_2 \in \text{Hom}(V,W)$

$(T_1 + T_2)(v) = T_1(v) + T_2(v)$

$= T_2(v) + T_1(v)$

$= (T_2 + T_1)(v)$

$T_1(v), T_2(v) \in W$ & W is vector space $\therefore$ abelian group under addition

$\therefore$ $X = (\text{Hom}(V,W), +)$ is an abelian group

Define $X \cdot F \longrightarrow X$

$T \cdot \alpha = \alpha T$

where $\alpha T(v) = \alpha(T(v))$

Now is $\alpha T \in X$

$(\alpha T)(\beta v_1 + v_2) = \alpha(T(\beta v_1 + v_2))$

$= \alpha(\beta T(v_1) + T(v_2))$

$= \alpha\beta T(v_1) + \alpha T(v_2)$

$1 \cdot T = T$

DATE: / / 20
PAGE No.

$= \beta \alpha T(v_1) + \alpha T(v_2)$

$= \beta(\alpha T)(v_1) + (\alpha T)(v_2)$

$\Rightarrow \alpha T \in X$

* Now $(\alpha+\beta)T = \alpha T + \beta T \quad \forall\ \alpha, \beta \in f$

$((\alpha+\beta)T)(v) = (\alpha+\beta)T(v)$

$= \alpha T(v) + \beta T(v)$

as $\alpha, \beta \in f$, $T(v) \in W$, W is vector space $\Rightarrow (\alpha+\beta)w = \alpha w + \beta w \ \forall\ w \in W$

$= \alpha T(v) + \beta T(v)$

$= \alpha T + \beta T$

* $(\alpha \cdot \beta) \cdot T = \alpha \cdot (\beta \cdot T) \quad \forall\ \alpha, \beta \in f$

$(\alpha \cdot \beta) \cdot T = ((\alpha \cdot \beta) \cdot T)(v)$

$= (\alpha \cdot \beta)(T(v))$

$= \alpha \cdot \beta \cdot T(v)$

$= \alpha(\beta T(v))$

$= \alpha(\beta T)$

as $T(v) \in W$, W is vector space, $\because \alpha, \beta \in f$, $w \in W$, $(\alpha\beta)w = \alpha(\beta w)$

* $\because \quad 1 \cdot T = T$

as $1 \in f$

$1.T = 1.T(v) = 1(T(v))$

$= T(v) = T$

$\therefore (Hom(V,W), +, \times)$ is a vector space over f

Linear functional

Let V be a vector space over f. Then any linear transformation $T: V \longrightarrow F$ is called a linear functional

F: vector space { every field is vector space over itself }

eg $T: \mathbb{R}^2 \longrightarrow \mathbb{R}$ defined by

$T(a,b) = a+b$

is linear functional

$T: \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ is not functional as codomain should be $\mathbb{R}$ for it to be functional

$T(a,b) = (b,a)$.

for linear check

$T(\alpha v_1 + v_2)$

$V^* = Hom(V, F)$ is a vector space

(linear functional collection)

↓ Dual space of V

* Every linear functional is L.T but converse may not be true

Let V_f be vector space
Then $V^* = \text{Hom}(V_f, f)$ is again a vector space over f

Theorem.

Let V be a finite dimensional vector space of dimension n. and its basis is $\{v_1, v_2 \dots v_n\}$ then V^* is also a vector space with dimension n & basis is $\{\phi_1, \phi_2 \dots \phi_n\}$ defined by

$$\phi_i : V \to f$$
$$\phi_i(\alpha_1 v_1 + \alpha_2 v_2 \dots \alpha_n v_n) = \alpha_i \quad \forall \ 1 \le i \le n$$

Proof Firstly we show that each ϕ_i is well defined

Let $v, w \in V$ s.t $v = w$

now $v = \alpha_1 v_1 + \alpha_2 v_2 \dots + \alpha_n v_n \quad \forall \ \alpha_i^\circ \in f$

$$w = \beta_1 v_1 + \beta_2 v_2 \dots + \beta_n v_n \quad \forall \ \beta_i^\circ \in f$$

$$\Rightarrow \alpha_1 v_1 + \alpha_2 v_2 \dots + \alpha_n v_n = \beta_1 v_1 + \beta_2 v_2 \dots + \beta_n v_n$$

$$\Rightarrow (\alpha_1 - \beta_1) v_1 + (\alpha_2 - \beta_2) v_2 + \dots + (\alpha_n - \beta_n) v_n = 0$$

but as $\{v_1, v_2 \dots v_n\}$ is linearly independent as it basis of V

$$\therefore \quad \alpha_i^\circ - \beta_i^\circ = 0 \quad \forall \ i \le i \le n$$

$$\Rightarrow \alpha_i^\circ = \beta_i^\circ \quad \forall \ i \le i \le n$$

$\Rightarrow \phi_i(v) = \phi_i(w) \quad \forall\ 1 \le i \le n$

Hence each ϕ_i is well defined

$$\phi_i(\alpha v + w) = \phi_i\left(\alpha(\alpha_1 v_1 + \alpha_2 v_2 \cdots \alpha_n v_n) + \beta_1 v_1 + \beta_2 v_2 + \cdots \beta_n v_n\right)$$

$$= \phi_i\left(\alpha\alpha_1 v_1 + \alpha\alpha_2 v_2 + \alpha\alpha_3 v_3 + \cdots \alpha\alpha_n v_n + \beta_1 v_1 + \beta_2 v_2 + \cdots \beta_n v_n\right)$$

$$= \phi_i\left((\alpha\alpha_1 + \beta_1) v_1 + (\alpha\alpha_2 + \beta_2) v_2 + \cdots (\alpha\alpha_n + \beta_n) v_n\right)$$

$$= \alpha\alpha_i + \beta_i$$

$$= \alpha\phi_i(v) + \phi_i(w)$$

$\therefore \phi$ is linear functional

$\Rightarrow \phi_i \in V^*$

<u>Claim</u> $\{\phi_1, \phi_2 \cdots \phi_n\}$ is linearly independent over f

clearly $\phi_i(v_j) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$

Let $\beta_1, \beta_2 \cdots \beta_n \in f$ s.t

$$\beta_1\phi_1 + \beta_2\phi_2 + \cdots \beta_n\phi_n = 0$$

$\Rightarrow (\beta_1\phi_1 + \beta_2\phi_2 + \dots \beta_n\phi_n)(v_i) = 0 \quad \forall\ 1 \le i \le n$

$\Rightarrow \beta_1\phi_1(v_i) + \beta_2\phi_2(v_i) + \dots \beta_n\phi_n(v_i) = 0$

$\Rightarrow \beta_i = 0 \quad \forall\ 1 \le i \le n$

Hence $\{\phi_1, \phi_2 \dots \phi_n\}$ is linear independent over f

claim Span $\{\phi_1, \phi_2, \dots \phi_n\} = V^*$

Let $f \in V^*$

$\Rightarrow f: V \to F$ is a linear functional

Let $f(v_i) = a_i$ for some $a_i \in F$

claim $\exists$ some scalars $r_1, r_2, \dots r_n$ s.t
$r_1\phi_1 + r_2\phi_2 + \dots r_n\phi_n = f$

i.e $\exists$ some scalars $r_1, r_2 \dots r_n$ s.t

$(r_1\phi_1 + r_2\phi_2 \dots r_n\phi_n)(v_i) = f(v_i) \quad \forall\ 1 \le i \le n$

$\Rightarrow r_1\phi_1(v_1) + r_2\phi_2(v_2) + \dots r_n\phi_n(v_i) = a_i \quad \forall\ 1 \le i \le n$

$\Rightarrow r_i = a_i \quad \forall\ 1 \le i \le n$

$\Rightarrow$ we can take $a_1\phi_1 + a_2\phi_2 + \dots a_n\phi_n \in \text{span}\{\phi_1, \phi_2 \dots \phi_n\}$

s.t $a_1\phi_1 + a_2\phi_2 + \cdots a_n\phi_n = f$

Q. Let $B = \{(2,1), (3,1)\}$ be basis of $_{\mathbb{R}}\mathbb{R}^2$. find basis of $_{\mathbb{R}}\mathbb{R}^{2*}$

Let $\{\phi_1, \phi_2\}$ be basis of $\mathbb{R}^{2*}$

$\phi_1(v_1) = 1 \qquad \phi_1(v_2) = 0$

$\phi_2(v_1) = 0 \qquad \phi_2(v_2) = 1$

$\Rightarrow \phi_1(2,1) = 1 \qquad \phi_1(3,1) = 0$

$\phi_2(2,1) = 0 \qquad \phi_2(3,1) = 1$

$\phi_i : \mathbb{R}^2 \to F$

$\phi_1(2,1) \in F$

$\phi_1(x_1, x_2) = [a\ b]\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = ax_1 + bx_2$ (by some theorem of Linear alg I)

$\Rightarrow \phi_1(2,1) = 1 \qquad \phi_1(3,1) = 0$

$\Rightarrow 2a + b = 1 \qquad \Rightarrow 3a + b = 0$

$\phi_2(2,1) = 0$ $\quad$ $\phi_2(3,1) = 1$

$2c+d = 0$ $\quad$ $3c+d = 1$

solving $\quad a=-1 \quad b=3$
$\quad\quad\quad\quad c=1 \quad d=-2$

as $\boxed{\phi_1(x,y) = ax+by}$

$\therefore \phi_1(x,y) = -x+3y$

$\boxed{\phi_2(x,y) = cx+dy}$

$\phi_2(x,y = x-2y$

$\{\phi_1, \phi_2\}$ is basis of $\mathbb{R}^2$ & is called dual ~~basis of~~ to given basis

Corollary Let V be a finite dimensional vector space over $\mathbb{R}$. Let $(0 \neq) v \in V$. Then $\exists\ f \in V^*$ s.t $f(v) \neq 0$

Proof as $v \neq 0$
$\Rightarrow \{v\}$ is a linearly independent set

$\Rightarrow \{v\}$ can be extended to a basis of V

Let claim $\dim V = n$ and
$\{v = v_1, v_2, \ldots v_n\}$ be basis of V

let $\{\phi_1, \phi_2 \ldots \phi_n\}$ be basis of V^* dual to basis B of V

$\Rightarrow \quad \phi_1(v_1) = 1$

$\Rightarrow \quad \phi_1(v_1) \neq 0$
$\Rightarrow \quad \phi_1(v) \neq 0$

Theorem: Let V be a finite dimensional space over f define $\theta : V \longrightarrow V^{**}$ by
$\theta(v) = T_v \quad \forall \ v \in V$

where $T_v : V^* \longrightarrow f$ s.t

$$T_v(f) = f(v) \quad \forall \quad f \in V^*$$

Then θ is an isomorphism from V to V^{**}

Proof: claim $T_v \in V^{**} = \text{Hom}(V^*, f)$
i.e T_v is a linear transformation from V^* to f

i.e T.P ① $T_v(f+g) = T_v(f) + T_v(g) \quad \forall f, g \in V^*$
② $T_v(\alpha f) = \alpha T_v(f) \quad f \in V^*, \alpha \in f$

$T_v(f+g) = (f+g)(v)$ { by def^n of T_v }

$= f(v) + g(v)$

$= T_v(f) + T_v(g)$ { $\because$ f is itself linear transformation }

$T_v(\alpha f) = (\alpha f)(v)$

$= \alpha(f(v))$

$= \alpha\, T_v(f)$

$\therefore T_v$ is linear transformation from $V^* \to F$

So $T_v \in V^{**}$

θ is well defined

Let $v_1, v_2 \in V$ s.t

$v_1 = v_2$

T.P $\theta(v_1) = \theta(v_2)$

i.e $T_{v_1} = T_{v_2}$

$T_{v_1}(f) = T_{v_2}(f)$ for all $f \in V^*$

i.e $f(v_1) = f(v_2)$

which is true as f is well defined (as $f \in V^*$)

$\therefore$ θ is well defined

DATE : / 20
PAGE No

claim θ is a linear transformation

To show $\theta(v_1+v_2) = \theta(v_1)+\theta(v_2) \quad \forall\ v_1, v_2 \in V$

$\theta(\alpha v) = \alpha\theta(v) \quad \forall\ v \in V \ \& \ \alpha \in f$

$\theta(v_1+v_2) = T_{v_1+v_2}$

$T_{v_1+v_2}(f) = f(v_1+v_2)$ {f is Linear transf.}

$= f(v_1) + f(v_2)$

$= T_{v_1}(f) + T_{v_2}(f) \quad = (T_{v_1}+T_{v_2})(f)$

~~$= \theta(v_1) + \theta(v_2)$~~

$\Rightarrow T_{v_1+v_2} = T_{v_1} + T_{v_2}$

$\Rightarrow \theta(v_1+v_2) = \theta(v_1) + \theta(v_2)$

$\theta(\alpha v) = T_{\alpha v}$

$T_{\alpha v}(f) = f(\alpha v)$

$= \alpha f(v)$ {$\because f$ is Linear transfo

$= \alpha T_v(f)$

$= \alpha T_v(f)$

$\therefore T_{\alpha v} = \alpha T_v$

$\Rightarrow \theta(\alpha v) = \alpha\theta(v)$

One-One

Let $v \in \text{Ker}\theta$

$\Rightarrow \theta(v) = 0$

$\Rightarrow T_v = 0$

$\Rightarrow T_v(f) = 0 \quad \forall\ f \in V^*$

$= f(v) = 0$

$\Rightarrow v = 0$ { by previous corollary }

$\Rightarrow \text{Ker}\theta = \{0\}$

$\therefore \theta$ is 1-1

as Dimension of $V = V^* = V^{**}$

$\therefore$ dimension V = dim V^{**}

and θ is 1-1, so θ is onto

(by rank nullity theorem)

Annihilators

Defⁿ: Let W be a nonempty subset of a vector space V. A linear function $\phi \in V^*$ is called an annihilator of W if

$$\phi(w) = 0 \quad \forall\ w \in W.$$

$$\text{Ann}(W) = \{ \phi \in V^* ;\ \phi(w) = 0 \ \forall\ w \in W \}$$

eg $W = \{0\} \subseteq V^*$

$$\text{Ann}(W) = \{ \phi \in V^* ; \phi(w) = 0 \ \forall \ w \in W \}$$

$$= \{ \phi \in V^* ; \phi(0) = 0 \}$$

$$= V^*$$

if $W = \{ v(\neq 0) \}$

$W^0 = \text{Ann}(W) \subseteq V^*$

W^0 = Annihilator of W

Q $V = \mathbb{R}^2$ over $\mathbb{R}$ $\quad W = \{(1,1), (2,2)\}$

find Ann(W)

$\phi : \mathbb{R}^2 \to \mathbb{R}$

$\phi(x,y) = ax + by$

$\phi(1,1) = a + b = 0$

$\phi(2,2) = 2a + 2b = 0$

Result Let W be a non empty subset of a vector space V. Then $Ann(W)$ is a subspace of V^*

Proof As $0(v) = 0 \quad \forall \ v \in V$

$\Rightarrow 0(w) = 0 \quad \forall \ w \in W$

$\Rightarrow 0 \in Ann(W)$

$\Rightarrow Ann(W) \neq \phi$

Let $\phi, \psi \in Ann(W)$

$$(\phi - \psi)(w) = \phi(w) - \psi(w)$$
$$= 0 - 0$$
$$= 0 \qquad \forall \ w \in W$$

$\Rightarrow (\phi - \psi) \in Ann(W)$

Let $a \in F$, $\phi \in Ann(W)$

$$(a\phi)(w) = a\phi(w)$$
$$= a.0$$
$$= 0 \qquad \forall \ w \in W$$

$\Rightarrow a\phi \in Ann(W)$

Theorem Suppose V has finite dimension & W is a subspace of V then

① $\dim(W) + \dim(W^0) = \dim(V)$

② $W^{00} = W$ $\quad \{W^{00} = (W^0)^0\}$

Proof Let $\dim V = n$ & $\dim W = m \leq n$

Let $B = \{w_1, w_2 \ldots w_m\}$ be basis of W

So B is linearly independent set and it can be extended to a basis

$$B_1 = \{w_1, w_2, \ldots w_m, v_1, v_2 \ldots v_{n-m}\}$$
$$= \{u_1, u_2 \ldots \ldots u_n\}$$

Let $\{\psi_1, \psi_2, \ldots \psi_n\}$ is a basis of V^* dual to basis B_1 of V

where $\psi_1(w_1) = 1$, $\psi_i(w_i) = 0 \quad \forall \quad 2 \leq i \leq m$

$\psi_i(u_i) = 0 \quad \forall i$

i.e $\psi_i(u_j) = 0$ if $i \neq j$ & $\psi_i(u_j) = 1$ if $i = j$

Claim $\dim W^0 = n - m$

Let $\phi \in W^0 \Rightarrow \phi \in V^*$ $\quad \{W^0$ is subspace of $V^*\}$

as $\{\psi_1, \psi_2 \ldots \psi_n\}$ is a basis of V^* dual to basis $\{u_1, u_2 \ldots u_m\}$ of V

$\Rightarrow \phi = a_1\psi_1 + a_2\psi_2 + \ldots a_n\psi_n$ where

$a_i = \phi(v_i) \quad \forall \quad 1 \le i \le n$

$\Rightarrow \phi = \phi(u_1)\psi_1 + \phi(u_2)\psi_2 + \cdots \phi(u_n)\psi_n$

$= 0 + 0 + \cdots 0 + \phi(u_{m+1})\psi_{m+1} + \cdots \phi(u_n)\psi_n$

$= \phi(u_{m+1})\psi_{m+1} + \cdots \phi(u_n)\psi_n$

which is a linear combination of $\psi_{m+1}, \cdots \psi_n$

$\Rightarrow W^\circ$ is span of $\{\psi_{m+1}, \cdots \psi_n\}$

Also this is linearly independent set being the subset of L.I set $\{\psi_1, \psi_2 \cdots \psi_n\}$

$\Rightarrow \{\psi_{m+1}, \cdots, \psi_n\}$ is basis of W°

$\dim W^\circ = n-(m+1)+1$

$= n-m$

(ii) $(W^\circ)^\circ = W$ $\quad \{W^\circ = \{\phi \in V^* \ \phi(w)=0 \ \forall \ w \in W\}$

$(W^\circ)^\circ = \{\phi \in V^{**} \ \phi(w)=0 \ \forall \ w \in W^\circ\}$

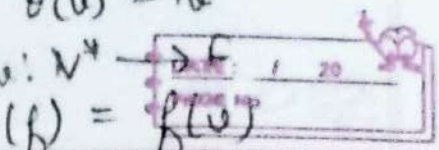
Let $\dim W = m$

$\dim W^\circ = n-m$ $\quad \{\dim(V) = n\}$

$\dim (W^\circ)^\circ = n-(n-m)$ $\quad \{\because \dim(V^*)=n\}$

$= m$

$$\begin{cases} \theta(v) : V \to V^{**} \\ \theta(v) = T_v \\ T_v : V^* \to F \\ T_v(f) = f(v) \end{cases}$$



claim $W \subseteq W^{\circ\circ}$

let $w \in W$

claim $T_w \in W^{\circ\circ}$

let $f \in W^\circ$

$T_w(f) = f(w) = 0$

$\Rightarrow T_w(f) = 0 \quad \forall f \in W^\circ$.

~~$f \in W^\circ$~~ $\Rightarrow T_w \in W^{\circ\circ}$

8 let U and W be subspaces of V . Prove that $(U+W)^\circ = U^\circ \cap W^\circ$