If I feel unhappy, I do mathematics to become happy. If I am happy, I do mathematics to keep happy.

- PAUL TURAN -

Euclidean Domains and Unique Factorisation Domains

→ The division algorithm in the ring of integers is the motivation for the class of rings, namely, Euclidean rings.

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

(i) $\forall\, a, b \in R,\ a \neq 0,\ b \neq 0 ;\ d(a) \leq d(ab)$ and

(ii) for any $a, b \in R,\ b \neq 0$ there exist $q, r \in R$ such that $a = bq + r$ where either $r = 0$ or $d(r) < d(b)$

Note:

1. For any $a(\neq 0) \in R$, $d(a) \geq 0$.
2. For the zero element 0 of R, $d(0)$ is not defined. However some authors defined $d(0) = 0$, integer.
3. The property (ii) in the above definition is called division algorithm.
4. From the above definition we note that $d : R - \{0\} \longrightarrow Z$ is a mapping such that

(i) $d(a) \geq 0 \quad \forall a \in R - \{0\}$

(ii) $d(a) \leq d(ab)$ for all $a, b \in R - \{0\}$ and

(iii) there exist $q, r \in R$ s.t that $a = bq + r$ where either $r = 0$ or $d(r) < d(b)$ for any $a \in R$, $b \in R - \{0\}$

Example (1): Show that the ring Z of integers is an Euclidean ring.

Soln: Given that the ring $(Z, +, \times)$ of integers is an integral domain.

Let us define the mapping $d : Z - \{0\} \longrightarrow Z$

by $d(a) = |a| \quad \forall a \in Z - \{0\}$ ——— (1)

(i) Since $|a| > 0$,
we have $d(a) \geq 0 \quad \forall a \in Z - \{0\}$.

(ii) For $a \neq 0, b \neq 0$ in Z, $ab \neq 0$ in Z.

$$\therefore d(ab) = |ab|$$
$$= |a||b|$$
$$\geq |a| \quad (\because |b| \geq 1)$$
$$= d(a)$$

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

(iii) For $a, b \in Z, b \neq 0$; by division algorithm in integers,

$\exists\ q, r \in Z$ such that $a = bq + r$, where $0 \leq r < |b|$

i.e, $a = bq + r$, where $r = 0$ or $0 < r \leq |b|$

i.e, $a = bq + r$, where $r = 0$ or $d(r) < d(b)$.

$\therefore (Z, +, \times)$ is an Euclidean ring.

Example (2): Show that the ring of Gaussian integers is an Euclidean ring.

Soln: Given that $Z[i] = \{ a + ib \mid a, b \in Z, \ i = \sqrt{-1} \}$ of Gaussian integers is an integral domain w.r.t $+^n$ and $\times^n$.

Let us define the mapping $d: Z[i]-\{0\} \to Z$ by $d(x+iy) = x^2+y^2 \ \forall\ x+iy \in Z[i]-\{0\}$.

i.e $d(x+iy) = |x+iy|^2$

$= x^2+y^2 \ \forall\ x+iy \in Z[i]-\{0\}$ ——— (1).

we have $x \neq 0$ or $y \neq 0$ and hence $x^2+y^2 \geq 1$.

$\therefore d(z) = d(x+iy) \geq 0 \ \forall\ z \in Z[i]-\{0\}$.

Let $z_1, z_2 \in Z[i]-\{0\}$ then we have $z_1 = a+ib$, $z_2 = c+id$ where $a,b,c,d \in Z$ and $a \neq 0$ or $b=0$; $c \neq 0$ or $d \neq 0$.

$\therefore z_1 z_2 = (ac-bd)+i(ad+bc)$.

Now we have $d(z_1 z_2) = (ac-bd)^2+(ad+bc)^2$

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

$\geq a^2+b^2 = d(z_1)$

$(\because c^2+d^2 \geq 1)$

$\therefore \boxed{d(z_1) \leq d(z_1 \cdot z_2).}$

Now we have

$$\frac{z_1}{z_2} = \frac{a+ib}{c+id}$$

$$= \frac{ac+bd}{c^2+d^2} + i\left[\frac{bc-ad}{c^2+d^2}\right]$$

$$\frac{z_1}{z_2} = p+iq \ (\text{say})$$

where $p = \frac{ac+bd}{c^2+d^2}$; $q = \frac{bc-ad}{c^2+d^2}$ are rational numbers.

Corresponding to the rational numbers p and q, we can find suitable integers p' and q' such that-

$|p'-p| \le \frac{1}{2}$ and $|q'-q| \le \frac{1}{2}$

Let $t = p' + q'i$ then $t \in Z[i]$

and $\frac{z_1}{z_2} = \lambda$, where $\lambda = p + qi$

$\Rightarrow z_1 = \lambda z_2$

$= (\lambda - t) z_2 + t z_2$

$\boxed{z_1 = t z_2 + r}$ where $r = (\lambda - t) z_2$

NOW $z_1, z_2, t \in Z[i]$

$\Rightarrow z_1 - t z_2 \in Z[i]$

$\Rightarrow r \in Z[i]$.

$\therefore \exists\ t, r \in Z[i]$ s.t $z_1 = t z_2 + r$ where

$r = 0$, or

$d(r) = d[(\lambda - t) z_2]$

$= d[(p+qi) - (p'+q'i)] d(z_2)$

$= d[(p-p') + (q-q')i] d(z_2)$.

$= [(p-p')^2 + (q-q')^2] d(z_2)$.

$\le \left[\frac{1}{4} + \frac{1}{4}\right] d(z_2)$

$= \frac{1}{2} d(z_2)$

$< d(z_2)$.

Thus $\exists\ t, r \in Z[i]$ s.t $z_1 = t z_2 + r$

where $r = 0$ (or) $d(r) < d(z_2)$.

Note :- from the definition of Euclidean domain, that ∃ a non-negative integer $d(a)$ for any $a \neq 0$, we mean, ∃ a function d from $R-\{0\}$ to $Z^+ \cup \{0\}$, where Z^+ is the set of +ve integers.

This function d is called **Euclidean valuation** on R.

Also the last condition in the definition is called Euclidean algorithm.

→ Every field is a Euclidean ring.

Soln: Let F be a field and F^* be the set of all non-zero elements of F.

Since F is a field, so F is an integral domain.

Define the mapping $d: F^* \to Z$ by

$d(a) = 0$ (zero integer) $\forall\, a \in F^*$ ——— (1)

$\therefore d(a) \geq 0 \quad \forall a \in F^*$

Let $a, b \in F^*$

Then a, b and ab are non-zero elements of F.

$\therefore d(a) = 0$ and $d(ab) \geq 0$ (from (1))

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

Let $a \in F$ and $b \in F^*$

Now $a = a1$, where '1' is the unity element of F.

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

$= (ab^{-1})b$

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

where '0' is the zero element of the field F.

$\therefore a = bq + r$ where $q = ab^{-1}$, $r = 0$.

Hence for $a \in F$, $b \in F^*$ there exist $q, r \in F$ such that $a = qb + r$ where $r = 0$

$\therefore$ F is an Euclidean ring.

Note: we can prove the above theorem by defining

$d : F^* \longrightarrow \mathbb{Z}$ by $d(a) = 1$ (integer) $\forall a \in F^*$.

⊗ The field $\mathbb{Q}$ of rational numbers with $d(a) = 1$ for all $a \neq 0 \in \mathbb{Q}$ is a Euclidean domain. However, $\mathbb{Q}$ with $d(a) = |a|$, for all $a \neq 0 \in \mathbb{Q}$, is not a Euclidean domain.

Sol": If $d(a) = 1$ $\forall a \neq 0 \in \mathbb{Q}$, then $\mathbb{Q}$ is a Euclidean domain.

However, $\mathbb{Q}$ with $d(a) = |[a]|$ $\forall a \neq 0 \in \mathbb{Q}$ is not a Euclidean domain,

Taking $a = \frac{3}{2}$; $b = \frac{2}{3}$; $\frac{3}{2} = \left|\frac{3}{2}\right| > 1 = \left|\frac{3}{2} \cdot \frac{2}{3}\right| = d(a \cdot b)$.

$\therefore d(a) = 2$; $d(a \cdot b) = 2$

$\therefore d(a) \not< d(a \cdot b)$ ⟶ a contradiction.

→ Show that $\mathbb{Z}[\sqrt{2}] = \{ m+n\sqrt{2} : m, n \in \mathbb{Z} \}$ is a Euclidean domain.

Soln: We know that $\mathbb{Z}[\sqrt{2}]$ is an integral domain with unity $1 = 1 + \sqrt{2}\cdot 0$.

Let us define a mapping

$d : \mathbb{Z}[\sqrt{2}] - \{0\} \longrightarrow \mathbb{Z}$ by

$d(m+n\sqrt{2}) = |m^2 - 2n^2|$ $\forall\ m+n\sqrt{2} \in \mathbb{Z}[\sqrt{2}] - \{0\}$.

we have $m \neq 0$ or $n \neq 0$.

$\therefore d(m+n\sqrt{2})$ is a +ve integer.

for each $m+n\sqrt{3} \in \mathbb{Z}[\sqrt{2}] - \{0\}$.

$\therefore d(m+n\sqrt{2}) \geq 0$.

Now let: $a = m+n\sqrt{2} \neq 0$, $b = m_1+n_1\sqrt{2} \neq 0$ in $\mathbb{Z}[\sqrt{2}]$;

$m \neq 0$ or $n \neq 0$; $m_1 \neq 0$ or $n_1 \neq 0$.

Then we have

$$ab = (mm_1 + 2nn_1) + (mn_1 + m_1 n)\sqrt{2}$$

and $d(ab) = |(mm_1 + 2nn_1)^2 - 2(mn_1 + m_1 n)^2|$

(by defn)

$$= |m^2m_1^2 + 4n^2n_1^2 - 2(m^2n_1^2 + m_1^2n^2)|$$

$$= |(m^2 - 2n^2)(m_1^2 - 2n_1^2)|$$

$$= |m^2 - 2n^2|\,|m_1^2 - 2n_1^2|.$$

$$\geq |m^2 - 2n^2| \quad (\because |m_1^2 - 2n_1^2| \geq 1).$$

$\therefore = d(a)$.

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

Now we have

$$\frac{a}{b} = \frac{m+n\sqrt{2}}{m_1+n_1\sqrt{2}} = \frac{(m+n\sqrt{2})(m_1-n_1\sqrt{2})}{(m_1+n_1\sqrt{2})(m_1-n_1\sqrt{2})}$$

$$= \left(\frac{mm_1-2nn_1}{m_1^2-2n_1^2}\right) + \left(\frac{m_1n-mn_1}{m_1^2-2n_1^2}\right)\sqrt{2}$$

$$= p+q\sqrt{2}$$

where $p = \frac{mm_1-2nn_1}{m_1^2-2n_1^2}$ & $q = \frac{m_1n-mn_1}{m_1^2-2n_1^2}$ are rational numbers.

corresponding to the rational numbers p and q, we can find two integers p' and q' such that $|p'-p| \leq \frac{1}{2}$ and $|q'-q| \leq \frac{1}{2}$.

Let $t = p'+q'\sqrt{2}$.

Then $t \in \mathbb{Z}[\sqrt{2}]$

we have $\frac{a}{b} = \lambda$, where $\lambda = p+q\sqrt{2}$

$$\Rightarrow a = \lambda b = (\lambda - t)b + tb$$

$$= tb + r, \text{ where } r = (\lambda - t)b$$

Now $a, b, t \in \mathbb{Z}[\sqrt{2}]$

$\Rightarrow a - tb \in \mathbb{Z}[\sqrt{2}]$

$\Rightarrow r \in \mathbb{Z}[\sqrt{2}]$

$\therefore\ \exists\ t, r \in \mathbb{Z}[\sqrt{2}]$ such that

$a = tb + r$; where $r = 0$ (or)

$$d(r) = d\{(a-b)b\}$$

$$= d\{(p+q\sqrt{2}) - (p'+q'\sqrt{2})\}\, d(b)$$

$$= d\{(p-p') + (q-q')\sqrt{2}\}\, d(b).$$

$$= |(p-p')^2 - 2(q-q')^2|\, d(b)$$

$$\leq |(p-p')^2 + 2(q-q')^2|\, d(b)$$

$$\leq \left(\frac{1}{4} + \frac{2}{4}\right) d(b)$$

$$= \frac{3}{4}\, d(b)$$

$$< d(b).$$

$\therefore \mathbb{Z}[\sqrt{2}]$ is a Euclidean domain.

HW → Show that $\mathbb{Z}[\sqrt{3}] = \{m+n\sqrt{3} : m, n \in \mathbb{Z}\}$ is a Euclidean domain

→ Every Euclidean ring is a principal ideal ring.

(or)

Every ideal of an euclidean ring is a principal ideal.

Proof Let R be an euclidean ring.

Let U be an ideal of R.

TO prove that U is principal ideal.

Let $U=\{0\}$, where $'0' \in R$.

Then $U=\{0\}$ is the ideal generated by $'0' \in R$.

$\therefore U$ is a principal ideal of R.

Let $U \neq \{0\}$ then U contains non-zero elts.

Then $\exists\ x \in U (\subseteq R)$ and $x \neq 0$ s.t the set $\{d(x) / x \neq 0\}$ is a non-empty set of non-negative integers.

$\therefore$ By well ordering principle there exists $b \neq 0 \in U$ s.t $d(b) \leq d(x)$ where $x \neq 0 \in U$.

Now we prove that $U = \langle b \rangle$.

Let $a \in U$

By division algorithm, $\exists\ q, r \in R$ s.t $a = bq + r$ where $r = 0$ (or) $d(r) < d(b)$.

Since $b \in U, q \in R \Rightarrow bq \in U$ ($\because U$ is an ideal)

Since $a \in U, bq \in U \Rightarrow a - bq = r \in U$.

if $r \neq 0$ then $d(r) < d(b)$ which contradiction to the fact $d(b) \leq d(x)\ \forall x \neq 0 \in U$.

$\therefore r = 0 \rightarrow$ Hence $a = bq$

$\therefore U = \{bq / q \in R\} = \langle b \rangle$. is the principal ideal generated by 'b' ($\neq 0$) in U.

Hence every ideal U of R is a principal ideal.

$\therefore R$ is a principal ideal ring.

Note: ① If U is an ideal of euclidean ring R then U is a principal ideal of R so that $U = \langle b \rangle$.

$= \{bq / q \in R\}$.

② The converse of the above theorem need not be true.

Ex:- $R = \left\{ a + b\left(\frac{1+\sqrt{19}\,i}{2}\right) \Big/ a, b \in Z \right\}$, the ring of complex numbers is a principal ideal ring but not euclidean. (It will clear in UFD)

→ Every Euclidean ring possesses unity element.

Sol": Let R be an Euclidean ring.

$\therefore R$ is a principal ideal ring.

$\therefore R$ is an ideal generated by some element c of the ring R so that

$R = (c) = \{cq / q \in R\}$

$\therefore c \in R \Rightarrow c = ce$ for some $e \in R$.

we now prove that $e \in R$ is the unity.

Let $x \in R$: Then $x = cd$ for some $d \in R$

Now $xe = (cd)e = (dc)e = d(ce) = dc = cd = x$ ($\because R$ is I.D)

$\therefore xe = x \ \forall x \in R$.

Hence $e \in R$ is the unity element.

corollary: $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$ are principal ideal domains.

* **Divisibility:-** Let R be a commutative ring and $a, b \in R$, if $\exists\ q \in R$ s.t $b = aq$ then we say that 'a' divides 'b'.

Note: (1) If 'a' divides 'b' then $a|b$.

(2) if a does not divide 'b' then $a \nmid b$.

(3) If 'a' divides 'b' then we say that 'a' is a divisor of 'b' or 'a' is a factor of 'b'.

(4) for $a, 0 \in R$.
we have $0 = a \cdot 0$
Therefore every element $a \in R$ is a divisor of factor of '0'.

(5) $a, b \in R$ and $a|b \Leftrightarrow b = aq$ for some $q \in R$.

For example:

(i) In the ring $\mathbb{Z}$ of integers,
$3|15$ and $3 \nmid 7$.

(ii) In the ring $\mathbb{Q}$ of rational numbers
$3|7$ because there exists $\frac{7}{3} \in \mathbb{Q}$
so that $7 = 3 \cdot \frac{7}{3}$.

→ If R is a commutative ring with unity and $a, b, c \in R$ then (1) $a|a$ (2) $a|b, b|c \Rightarrow a|c$ (3) $a|b \Rightarrow a|bx$ $\forall x \in R$ and (4) $a|b, a|c \Rightarrow a|bx+cy$ $\forall x, y \in R$.

Prof: ① If $1 \in R$ is the unity element then we have $a = a1$.

Therefore a/a.

② $a/b \Rightarrow b = aq_1$ for some $q_1 \in R$

$b/c \Rightarrow c = bq_2$ for some $q_2 \in R$

$\therefore c = bq_2 = (aq_1)q_2 = a(q_1 q_2) = aq$

where $q = q_1 q_2 \in R$

$\therefore a/c$.

③ $a/b \Rightarrow b = aq$ for some $q \in R$

Now $bx = (aq)x = a(qx) = aq'$

where $q' = qx \in R$

$\therefore a/bx$.

④ $a/b \Rightarrow a/bx \Rightarrow bx = aq_1$ for some $q_1 \in R$

$a/c \Rightarrow a/cy \Rightarrow cy = aq_2$ for some $q_2 \in R$

Now $bx + cy = aq_1 + aq_2$

$= a(q_1 + q_2)$

$= aq$, where $q = q_1 + q_2 \in R$.

$\therefore a/bx + cy$

Note: a/b, $a/c \Rightarrow a/b+c$ and $a/b-c$.

Units:

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

In other words units of R are those elements of R which possess multiplicative inverse.

Finally, be careful not to confuse a unit with the unit element or the unity element of the ring. There may be more than one units in a ring but the unity element is always unique. Of course the unity element 1 is also one of the units.

Examples:

① ± 1 are the units in I (all integers).
(∵ These are only the invertible elements of the ring of integers).

② $\pm 1, \pm i$ are the units in $Z[i] = \{a+ib / a, b \in Z\}$. Herere $i = \sqrt{-1}$.

$\left(\because 1(1) = 1,\ (-1)(-1) = 1 \text{ and } i(-i) = 1\right)$.

→ $a \in R$ is a unit of $R \Rightarrow ab = 1$ for some $b \in R$, so $b \in R$ is also a unit of R.

→ If a, b are two units in R, then ab is also a unit in R.

Examples:

(1) In the ring Z of integers, we have
$1 \cdot 1 = 1$ and $(-1)(-1) = 1$ only.
1 and −1 are the only units in Z.

(2) If R is a field then every non-zero element of R has multiplicative inverse.
So, every non-zero element of a field is unit.

(3) $3+2\sqrt{2}$ is a unit in the domain -
$\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} / a, b \in \mathbb{Z}\}$

For, $3, -2 \in \mathbb{Z}$ we have
$3-2\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ so that $(3+2\sqrt{2})(3-2\sqrt{2}) = 1$.
where $1 \in \mathbb{Z}[\sqrt{2}]$ is the unity element.

Also every integral power of $3+2\sqrt{2}$ is also a unit of $\mathbb{Z}[\sqrt{2}]$.
Thus $\mathbb{Z}[\sqrt{2}]$ has infinite number of distinct units.

→ Let a, b be two non-zero elements of an Euclidean ring R. Then (1) if b is a unit in R, $d(ab) = d(a)$ and
(2) if b is not a unit in R, $d(ab) > d(a)$.

Proof: By definition of Euclidean ring,

$$d(ab) \geq d(a) \quad \text{---------- (1)}$$

(1) b is a unit in R ⇒ there exists $c \in R$ such that

$bc = 1$.

By the definition of Euclidean ring,

$$d((ab)c) \geq d(ab)$$

i.e, $d(a(bc)) \geq d(ab)$

i.e, $d(a1) = d(a) \geq d(ab)$ ——— (2)

From (1) and (2): $d(ab) = d(a)$.

(2) Let 'b' be not a unit in R.

$a \neq 0$, $b \neq 0 \in R$ and R is integral domain

$\Rightarrow ab(\neq 0) \in R$

By the division algorithm, there exist $q, r \in R$ such that (BA-1) $a = q(ab) + r$ where either $r = 0$ or $d(r) < d(ab)$.

If $r = 0$, $a = q(ab)$ i.e, $a = a(qb)$

i.e., $a(1 - qb) = 0$

Since R is an integral domain and $a \neq 0$ we have $1 - qb = 0$ i.e., $qb = 1$ which implies that b is a unit in R.

$\therefore r \neq 0$ and hence $d(r) < d(ab)$

i.e., $d(a - q(ab)) < d(ab)$

i.e., $d(a(1 - qb)) < d(ab)$

But $d(a(1 - qb)) \geq d(a)$ by the definition.

$\therefore d(a) \leq d(a(1 - qb)) < d(ab)$

Hence $d(a) < d(ab)$.

→ A non-zero element 'a' of a Euclidean ring R is unit $\Leftrightarrow d(a) = d(1)$.

Sol| Let $a (\neq 0) \in R$ be a unit in R

$\therefore \exists\ b \in R$ s.t $ab = 1$.

$\therefore d(1) = d(ab) \geq d(a)$. (by the definition of Euclidean ring) ——— (1)

Also $d(1a) \geq d(a)$ (by defn of ED)

$\Rightarrow d(a) \geq d(1)$ ——— (2)

$\therefore$ from (1) and (2) we have $d(a) = d(1)$.

Conversely, let $d(a) = d(1)$

TO P.T $a (\neq 0)$ is a unit in R

If possible let a is not unit in R

Then $d(a) = d(1a) > d(1)$ (by definition of ED)

$\Rightarrow d(a) > d(1)$

This is a contradiction.

Hence 'a' must be a unit in R.

*Associates :-

Let R be a commutative ring with unity.

An element $a \in R$ is said to be an associate of $b \in R$ if $a = bu$ where u is a unit in R.

Note :- (1) The relation of being associates is an equivalence relation in R. So, if $a \in R$ is an associate of $b \in R$, by the property of symmetry, $b \in R$ is an associate of $a \in R$.

Therefore two elements $a, b \in R$ are associates in R if $a = bu$ where u is a unit in R.

(2) If a, b are associate in R then $a = bu$ where u is a unit in R. Therefore,

$$d(a) = d(bu) = d(b).$$ (by previous theorem proved after)

(3) If 'a' is an unit of the ring R and 1 is the unity element then $a = 1a$, so the unity element '1' is an associate of the unit 'a'.

for example : (1) In the ring Z of integers the units are 1, -1 only.

for $a \in Z$, we have $a = a \cdot 1$ & $a = (-a)(-1)$ only.

Therfore $a \in Z$ has only two associates $a, -a$.

(2) In the ring $Z_6 = \{0, 1, 2, 3, 4, 5\}$ of integers modulo 6, the units are 1, 5 only.

for $2 \in \mathbb{Z}_6$, we have $2 \equiv 2.1 \pmod 6$

and $2 \equiv 4.5 \pmod 6$

$\therefore$ 2 has two associates 2 and 4.

(3) 1 and $-i$ are associates in $\mathbb{Z}[i]$,
since $1 = (-i)(i)$, i being unit in $\mathbb{Z}[i]$.

(4) $2+3i$ and $2i-3$ are associates,
since $2i-3 = (2+3i)i$,
i being a unit in $\mathbb{Z}[i]$.

→ If a, b are two non-zero elements of an integral domain R with unity then a, b are associates in R if and only if a/b and b/a.

Sol^n: Let a, b be associates in R.

Since 'a' is an associate of b,

$a = bu$ for some unit $u \in R$.

$\therefore b/a$.

Since 'b' is an associate of 'a',

$b = au'$ for some unit $u' \in R$.

$\therefore a/b$.

Conversely, let a/b and b/a.

$\therefore b = aq_1$ and $a = bq_2$ for some $q_1, q_2 \in R$.

$\therefore b = aq_1 = (bq_2)q_1 = b(q_2 q_1)$

$\Rightarrow b(1 - q_2 q_1) = 0$

Since $b \neq 0$ and R is an integral domain.

we have

$1 - q_2 q_1 = 0$

$\Rightarrow q_2 q_1 = 1$.

$\therefore q_2$ is a unit in R.

$\therefore a = bq_2$ where q_2 is a unit in R.

Hence a, b are associates in R.

→ **Greatest Common Divisor:**

Let R be a commutative ring and a, b be any two non-zero elements of R. A non-zero element $d \in R$ is called a highest common factor (h.c.f) or a greatest common divisor (g.c.d) of a and b if (i) $d|a$ and $d|b$

(ii) whenever $c \neq 0 \in R$ is such that $c|a$ and $c|b$, then $c|d$.

g.c.d of a and b is denoted by (a, b).

Least Common Multiple: Let R be a commutative ring and a, b be any two non-zero elements of R. A non-zero element $c \in R$ is called a least common multiple (l.c.m) of a and b, if

(i) $a|c$ and $b|c$.

(ii) whenever $x \neq 0 \in R$ is such that $a|x$ and $b|x$, then $c|x$.

l.c.m of a and b is denoted by $[a, b]$.

Note: Any two non-zero elements of a ring may or may not have a g.c.d. (l.c.m). They may even have more than one g.c.d. (l.c.m).

Examples:

(1) → In $\mathbb{Z}$, 2 is a g.c.d of 4 and 6. Also -2 is a g.c.d of 4 and 6. further 12 is an l.c.m. of 4 and 6. Similarly -12 is also l.c.m of 4 and 6.

(2) → In the ring E of even integers, 4 and 6 do not have a g.c.d;
Notice that $2 \in E$ is not a g.c.d of 4 and 6,
Since $2 \cdot 2 = 4 \Rightarrow 2 \mid 4$ in E, but $2 \cdot 3 = 6 \Rightarrow 2 \nmid 6$ in E ($\because 3 \notin E$)

Similarly, 4 and 6 do not have a l.c.m.
Notice that $12 \in E$ is not a l.c.m. of 4 and 6,
since $4 \nmid 12$ in E ($\because 12 = 4 \cdot 3$ and $3 \notin E$).

(3) → In $\mathbb{Z}$, 6 is a g.c.d of 18 and 48.
Another g.c.d of 18, 48 is -6.

(4) → Consider the ring.
$\mathbb{Z}_{12} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{10}, \bar{11}\}$ of residue classes modulo 12;
Consider $\bar{6}, \bar{8} \in \mathbb{Z}_{12}$
since $\bar{6} = \bar{3} \cdot \bar{2}$ and $\bar{8} = \bar{4} \cdot \bar{2}$;
$\bar{2}$ is a common divisor of $\bar{6}, \bar{8}$.
If $\bar{x} \in \mathbb{Z}_{12}$ and $\bar{x} \neq \bar{0}$ then $\bar{x} \mid \bar{6}$, $\bar{x} \mid \bar{8}$.
$\Rightarrow \bar{x} \mid \bar{8} - \bar{6}$ i.e, $\bar{x} \mid \bar{2}$
$\therefore$ 2 is a g.c.d of $\bar{6}$ and $\bar{8}$.
Again $\bar{6} = \bar{10} \cdot \bar{3}$ and $\bar{8} = \bar{10} \cdot \bar{2}$.
$\Rightarrow \bar{10} \mid \bar{6}$ and $\bar{10} \mid \bar{8}$.
Let $\bar{x} \neq \bar{0} \in \mathbb{Z}_{12}$ be such that $\bar{x} \mid \bar{6}$ and $\bar{x} \mid \bar{8}$.

Then $\bar{x} \mid (\bar{5}\cdot\bar{8} - \bar{6})$ i.e., $\bar{x} \mid \bar{10}$

Thus $\bar{10}$ is also a g.c.d of $\bar{6}$ and $\bar{8}$

Now we show that $\bar{6}$ and $\bar{8}$ have no l.c.m.

Let $\bar{x}$ be an l.c.m of $\bar{6}$ and $\bar{8}$.

Then $\bar{6} \mid \bar{x}$ and $\bar{8} \mid \bar{x}$

Now $\bar{6} \mid \bar{x} \Rightarrow \bar{x} = \bar{6}\cdot\bar{y}$, for some $\bar{y} \in Z_{12}$

$\Rightarrow \bar{x} = \bar{0}$ or $\bar{6}$

$\Rightarrow \bar{x} = \bar{6}$ ($\because$ l.c.m is never zero)

It follows that $\bar{8} \mid \bar{6}$ and so $\bar{6} = \bar{8}\cdot\bar{z}$, for some $\bar{z} \in Z_{12}$

Consequently, $\bar{6} = \bar{8}\cdot\bar{z}$ is impossible.

Hence $\bar{6}$ and $\bar{8}$ have no l.c.m in Z_{12}.

Note: If d_1 d_2 are two g.c.d's of a, b then by the definition $d_1 \mid d_2$ and $d_2 \mid d_1$.

$\therefore d_1, d_2$ are associates of the ring.

Thus, in case of a g.c.d of a, b exists then it is unique apart from the distinction between associates.

In the above examples ①, ③ and ④

① $2, -2$ are associates in $\mathbb{Z}$

$12, -12$ are associates in $\mathbb{Z}$

③ & ④ $\bar{6}, -\bar{6}$ and $\bar{2}, \bar{10}$ are associates in $\mathbb{Z}$ and Z_{12} respectively.

In the ring $Z_8 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$, show that

(i) g.c.d $(\bar{4}, \bar{6}) = \bar{2}$ and $\bar{6}$

(ii) l.c.m $(\bar{4}, \bar{6}) = \bar{4}$

(iii) l.c.m $(\bar{3}, \bar{1}) = \bar{3}$ and $\bar{6}$.

→ Show that in Z_{20}, g.c.d. $(\bar{9}, \overline{18}) = \bar{9}$ and l.c.m. $(\bar{9}, \overline{18}) = \overline{18}$.

→ In the Euclidean ring R two elements 'a' and 'b' are said to be relatively prime if their greatest common divisor is a unit of R.

Since any associate of g.c.d is a g.c.d. and the unity element 1 is an associate of a unit.

a, b are relatively prime $\Leftrightarrow$ (a, b) = unit elt of R.

$\Leftrightarrow$ (a, b) = 1

$\Leftrightarrow$ ax + by = 1 for some $x, y \in R$.

→ Let 'a' be non-zero element of an integral domain R with unity element. If $b \in R$ is a divisor of 'a' but not an associate of 'a' then 'b' is a proper divisor of 'a'.

'b' is a proper divisor of 'a'.

$\Rightarrow$ a = bd where d is not a unit.

For any non-zero element 'a' of R, the units and associates of 'a' are divisors.

These are called improper divisors of 'a'.

Irreducible Element: Let R be a commutative ring with unity.

A non-zero and non-unit $p \in R$ is said to be an irreducible element, if p = ab implies that either a or b is a unit; $a, b \in R$. (in other words p has no proper factors)

Note: It may be observed that $p \in R$ is not irreducible, if there exists a pair of elements $a, b \in R$ such that $p = ab$, where a and b are both non-unit elements of R.

Prime Elements: Let R be a commutative ring with unity. A non-zero, non-unit element $p \in R$ is called a prime element, if $p \mid ab$ $(a, b \in R)$ implies that either $p \mid a$ or $p \mid b$.

Ex: (1). In the ring Z of integers the units are 1 and -1 only. If $p \neq 0 \in Z$ and $p \neq \pm 1$ and $p = p \cdot 1$ or $p = (-p)(-1)$ only then p is prime element in Z.

(2). In the ring $Z[i]$ of Gaussian integers $1+i$ is a prime element.

Note:

(1) It may be observed that $p \in R$ is not prime, if there exists a pair of elements, $a, b \in R$ such that $p \mid ab$, but $p \nmid a$ and $p \nmid b$.

(2) Irreducible and prime elements in a commutative ring with unity are always non-zero and non-unit elements.

(3) In the ring Z of integers, every prime number is both a prime element and irreducible element.

(4) The field Q of all rational numbers has neither any irreducible element nor prime element, as every non-zero element of Q is a unit. Indeed such an assertion is true for any field.

→ In the ring $Z_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$, show that $\bar{2}$ is a prime element but not irreducible.

Soln: The only units in Z_6 are $\bar{1}, \bar{5}$.

Thus $\bar{2} \in Z_6$ is non-zero and non-unit element.

Let $\bar{2} / \bar{a}\bar{b}$, where $\bar{a}, b \in Z_6$.

Then $ab-2$ is divisible by 6

$\Rightarrow ab-2 = 6x$, for some $x \in Z$

$\Rightarrow ab = 2(1+3x)$

$\Rightarrow 2/ab$

$\Rightarrow 2/a$ or $2/b$

i.e., $\bar{2}/\bar{a}$ or $\bar{2}/\bar{b}$

Hence $\bar{2}$ is a prime element of Z_6.

We have $\bar{2} = \bar{2} \otimes_6 \bar{4}$

where neither $\bar{2}$ nor $\bar{4}$ is a unit.

Hence $\bar{2}$ is not an irreducible element of Z_6.

→ Show that $1+i$ is an irreducible element in $Z[i]$.

Soln: Clearly, $1+i$ is a non-zero and non-unit element of $Z[i]$.

Note that the units in $Z[i]$ are $\pm 1, \pm i$.

Let $(1+i) = (a+bi)(c+di)$

where $a+bi, c+di \in Z[i]$.

Taking conjugates on both sides, we get

$(1-i) = (a-ib)(c-id)$

On multiplying the respective sides of the above equations, we get

$$2 = (a^2+b^2)(c^2+d^2) \quad (\because i^2 = -1).$$

The above equation yields the following cases:

Case(1): $a^2+b^2 = 1$ and $c^2+d^2 = 2$

Case(2): $a^2+b^2 = 2$ and $c^2+d^2 = 1$.

In case(1), $a^2+b^2 = 1 \Rightarrow (a+ib)(a-ib) = 1$

$\Rightarrow a+ib$ is a unit.

In case(2), $c^2+d^2 = 1 \Rightarrow c+di$ is a unit.

Hence $1+i$ is an irreducible element of $\mathbb{Z}[i]$.

→ Let us concentrate our discussion on the ring

$\mathbb{Z}[\sqrt{-5}] = \{a+b\sqrt{-5} / a, b \in \mathbb{Z}\}$.

It is a subring (with identity) of the field of complex numbers.

Hence $\mathbb{Z}[\sqrt{-5}]$ is an integral domain.

* In the following, we show some interesting properties of elements of $\mathbb{Z}[\sqrt{-5}]$:

(1) 1 and -1 are the only units of $\mathbb{Z}[\sqrt{-5}]$.

We show that an element $a+b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ is a unit iff $a^2+5b^2 = 1$

Suppose $a+b\sqrt{-5}$ is a unit.

Then there exists an element $c+d\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ such that $(a+b\sqrt{-5})(c+d\sqrt{-5}) = 1$. ①

Taking conjugates on both sides,

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

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

$\therefore$ from (1) and (2), we have

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

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

Since $a, b, c, d \in \mathbb{Z}$, we find that-

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

Conversely, Suppose $a^2+5b^2=1$

Then $(a+b\sqrt{-5})(a-b\sqrt{-5}) = 1$.

Hence $(a+b\sqrt{-5})$ is a unit

Now if $a^2+5b^2=1$, then $a = \pm 1$ and $b=0$ as $a, b \in \mathbb{Z}$.

Hence it follows that 1 and -1 are the only units of $\mathbb{Z}[\sqrt{-5}]$.

(2) $1+\sqrt{-5}$, $1-\sqrt{-5}$, 3, 2 are irreducible elements in $\mathbb{Z}[\sqrt{-5}]$.

Now, we show that 3 is an irreducible element-

Let $3 = (a+b\sqrt{-5})(c+d\sqrt{-5})$; $a, b, c, d \in \mathbb{Z}$.

Taking conjugates on both the sides, we get

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

On multiplying the respective sides of the above equations, we get

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

Both the sides of the above equation are positive integers.

Consequently, we have the following cases:

case(1): $a^2+5b^2=1$ and $c^2+5d^2=9$

case(2): $a^2+5b^2=9$ and $c^2+5d^2=1$

case(3): $a^2+5b^2=3$ and $c^2+5d^2=3$

It is clear that case(3) is not possible in $\mathbb{Z}$.
(∵ there are no $a,b,c,d \in \mathbb{Z}$, for which $a^2+5b^2=3$ and $c^2+5d^2=3$).

case (1) is possible when $a=\pm 1$, $b=0$

$\Rightarrow a+b\sqrt{-5} = \pm 1$

which are units in $\mathbb{Z}[\sqrt{-5}]$.

Similarly, case (2) yields that $c+d\sqrt{-5} = \pm 1$, which are units in $\mathbb{Z}[\sqrt{-5}]$.

Hence 3 is an irreducible element of $\mathbb{Z}[\sqrt{-5}]$.

Similarly 2, $1+\sqrt{-5}$, $1-\sqrt{-5}$ are irreducible elements in $\mathbb{Z}[\sqrt{-5}]$.

(3) $\rightarrow$ $1+\sqrt{-5}$, $1-\sqrt{-5}$, 3, 2 are not prime elements in $\mathbb{Z}[\sqrt{-5}]$:

We know $\mathbb{Z}[\sqrt{-5}] = \{a+b\sqrt{-5} \mid a,b \in \mathbb{Z}\}$ is an integral domain with unity.

Now let $2+\sqrt{-5}$ and $2-\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$

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

(Since $3\cdot 3 = 9 \Rightarrow 3 \mid 9$.
but $9 = (2+\sqrt{-5})(2-\sqrt{-5})$
$\Rightarrow 3 \mid 6 \Rightarrow 3 = 2\cdot 3$
but $6 = 1+\sqrt{-5}, 1-\sqrt{-5}$)

obviously, 3 divides $(2+\sqrt{-5})(2-\sqrt{-5}) = 9$, but 3 doesnot divide $2+\sqrt{-5}$ and $2-\sqrt{-5}$, for if 3 divides $2+\sqrt{-5}$, then $2+\sqrt{-5} = 3(a+b\sqrt{-5})$ for some $a,b \in \mathbb{Z}$.

→ Give an example to show that in an integral domain, every irreducible element need not be prime.

→ Prove that $2+\sqrt{-5}$ is irreducible but not prime in $Z[\sqrt{-5}]$.

Hint: Let $2+\sqrt{-5} = (a+b\sqrt{-5})(c+d\sqrt{-5})$; $a, b, c, d \in Z$.

Then $2-\sqrt{-5} = (a-b\sqrt{-5})(c-d\sqrt{-5})$.

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

we can easily show that $2+\sqrt{-5}$ is an irreducible element of $Z[\sqrt{-5}]$.

further $2+\sqrt{-5}$ divides $3\cdot 3 = 9 = (2+\sqrt{-5})(2-\sqrt{-5})$,

but $2+\sqrt{-5}$ doesnot divide 3.

Hence 3 is not a prime element of $Z[\sqrt{-5}]$.

→ Prove that $2-\sqrt{-5}$ is irreducible but not prime in $Z[\sqrt{-5}]$.

→ Prove that $1+\sqrt{-3}$ is irreducible but not prime in $Z[\sqrt{-5}]$.

→ Prove that 5 is irreducible but not prime in $Z[\sqrt{-6}]$.

→ Prove that 2, $1\pm\sqrt{-3}$ are irreducible elements of $Z[\sqrt{-3}]$.

→ Prove that 2 is an irreducible but not a prime element of $Z[\sqrt{-3}]$.

Hint: $4 = (1+\sqrt{-3})(1-\sqrt{-3})$, 2 divides 4 but 2 doesnot divide both $1+\sqrt{-3}$ and $1-\sqrt{-3}$.

→ If p, q are prime elements in an integral domain R with unity such that p/q, then show that p and q are associates.

Soln: By definition, p and q are non-zero and non-units. Since p/q, $q = ap$, for some $a \in R$.

Since $q = q \cdot 1$, $q/q \Rightarrow q/ap$

$\Rightarrow q/a$ or q/p.

since q is prime.

If q/a, then $a = qx$ for some $x \in R$.

Thus $q = ap = qxp$

$\Rightarrow q \cdot 1 = qxp$

$\Rightarrow 1 = xp$ ($\because q \neq 0$ and R is an ID).

$\Rightarrow p/1 \Rightarrow p$ is a unit.

$\Leftarrow$ a contradiction.

Thus $q/p \Rightarrow p = qy$, for some $\in R$

$\therefore q = ap \Rightarrow q \cdot 1 = aqy$

$\Rightarrow q \cdot 1 = q \cdot ay$

$\Rightarrow 1 = ay$

$\Rightarrow a/1$

$\Rightarrow a$ is a unit.

where $q = ap$.

Hence p and q are associates.

→ Let R be an integral domain with unity. Show that every prime element of R is irreducible. However, the converse need not be true.

Soln: Let p be any prime element of R.
Then $p \neq 0$ and p is not a unit.
we have to show that p is irreducible.
Let $p = ab$, where $a, b \in R$.
we shall prove that either a or b is a unit.

we have $p \cdot 1 = ab$
$\Rightarrow p/ab$
$\Rightarrow p/a$ or p/b, since p is prime.

Let p/a. Then $a = pr$, for some $r \in R$ and so $p = ab \Rightarrow p = (pr)b$

$\Rightarrow p \cdot 1 - p(rb) = 0$
$\Rightarrow p(1 - rb) = 0$
$\Rightarrow 1 - rb = 0$, as $p \neq 0$
$\Rightarrow rb = 1$
$\Rightarrow b/1$
$\Rightarrow b$ is a unit.

Similarly, we can show that if p/b, then a is a unit.
Hence p is an irreducible element.
However, the converse need not be true.
i.e., an irreducible element in an integral domain may not be prime.

For example: 3 is an irreducible element of $\mathbb{Z}[\sqrt{-5}]$, but is not a prime element of $\mathbb{Z}[\sqrt{-5}]$.

→ Show that $\sqrt{-5}$ is an irreducible element of $\mathbb{Z}[\sqrt{-5}]$

Theorem 2.8.2. *Prove that any two non-zero elements a, b in a P.I.D. R have a g.c.d. Further if $d \in R$ is a g.c.d. of a and b, then $d = \lambda a + \mu b$; for some $\lambda, \mu \in R$.* [D.U., 1999, 97]

Proof. Let $A = \{xa + yb : x, y \in R\}$. ...(1)

We shall prove that A is an ideal of R. Clearly, A is non-empty, since $0 = 0 \cdot a + 0 \cdot b \in A$. Let $\alpha, \beta \in A$. Then

$$\alpha = x_1 a + y_1 b, \beta = x_2 a + y_2 b \; ; \quad \text{where} \quad x_1, y_1, x_2, y_2 \in R.$$

We have

$$\alpha - \beta = (x_1 a + y_1 b) - (x_2 a + y_2 b) = (x_1 - x_2)\, a + (y_1 - y_2)\, b,$$

where $x_1 - x_2 \in R, y_1 - y_2 \in R$.

Thus $\alpha - \beta \in A$. For any $r \in R$ and $\alpha \in A$, we have

$$\alpha r = (x_1 a + y_1 b)\, r = r\,(x_1 a + y_1 b), \text{ since } R \text{ is commutative}$$

$$= (rx_1)\, a + (ry_1)\, b \in A, \text{ since } rx_1 \in R, ry_1 \in R$$

Since R is commutative, $r\alpha = \alpha r \in A$.

Thus A is an ideal of R. Since R is a P.I.D., so

$$A = (d), \text{ for some } d \in A. \qquad ...(2)$$

Since $d \in A$, so by virtue of (1), we can write

$$d = \lambda a + \mu b \text{ for some } \lambda, \mu \in R. \qquad ...(3)$$

We now proceed to show that d is g.c.d. of a and b. We have

$$a = 1 \cdot a + 0 \cdot b \quad \text{and} \quad b = 0 \cdot a + 1 \cdot b.$$

$\Rightarrow a \in A$ and $b \in A$, by (1).

Using (2), $a = dx$ and $b = dy$; for some $x, y \in R$

$\Rightarrow d \mid a$ and $d \mid b$.

Let $c \in R$ be such that $c \mid a$ and $c \mid b$. Then

$$c \mid \lambda a \text{ and } c \mid \mu b \Rightarrow c \mid (\lambda a + \mu b) \Rightarrow c \mid d, \text{ by (3).}$$

Hence d is a g.c.d. of a and b and $d = \lambda a + \mu b$; $\lambda, \mu \in R$.

EXAMPLES

Example 2.8.6. *Let R be an integral domain with unity and a, b be any two non-zero elements of R. Show that*

(i) $a \mid b$ and $b \mid a$ iff $(a) = (b)$.

(ii) a and b are associates iff $(a) = (b)$.

Solution. (*i*) Let $a \mid b$ so that $b = ac$, for some $c \in R$.

Let $x \in (b)$ be arbitrary. Then $x = br$, for some $r \in R$

or $x = (ac)\, r = a\,(cr)$, where $cr \in R$

$\Rightarrow$ $x \in (a)\ \forall\ x \in (b)$.

Thus $a \mid b \Rightarrow (b) \subseteq (a)$.

Similarly, $b \mid a \Rightarrow (a) \subseteq (b)$.

Hence $a \mid b$ and $b \mid a \Rightarrow (a) = (b)$.

Conversely, $(a) = (b) \Rightarrow a \in (b) \Rightarrow a = bs$, for some $s \in R$

$\Rightarrow b \mid a$.

Again $(a) = (b) \Rightarrow b \in (a) \Rightarrow b = at$, for some $t \in R \Rightarrow a \mid b$.

Hence $(a) = (b) \Rightarrow a \mid b$ and $b \mid a$.

(*ii*) By Example 2.7.4, a and b are associates $\Leftrightarrow a \mid b$ and $b \mid a$.

By part (*i*), $a \mid b$ and $b \mid a \Leftrightarrow (a) = (b)$. Hence the result follows.

Example 2.8.7. *In a P.I.D., prove that any two greatest common divisors of a and b are associates.*

Solution. By Theorem 2.8.2, any two non-zero elements a and b in a P.I.D. R have a g.c.d. Let d_1 and $d_2 \in R$ be any two greatest common divisors of a and b. Then $d_1 \mid a$ and $d_1 \mid b$; $d_2 \mid a$ and $d_2 \mid b$.

Since d_1 is a g.c.d. of a and b, so $d_2 \mid a$ and $d_2 \mid b \Rightarrow d_2 \mid d_1$.

Since d_2 is a g.c.d. of a and b, so $d_1 \mid a$ and $d_1 \mid b \Rightarrow d_1 \mid d_2$.

Hence $d_1 \mid d_2$ and $d_2 \mid d_1 \Rightarrow d_1$ and d_2 are associates, by Example 2.8.6.

Example 2.8.8. *In a P.I.D., prove that any associate of a g.c.d. is a g.c.d.*

Solution. Let R be a P.I.D. and $d_1 \in R$ be a g.c.d. of $a, b \in R$.

Let $d_2 \in R$ be an associate of d_1. Then $d_1 = ud_2$, for some unit $u \in R$. It follows that $d_2 \mid d_1$, where $d_1 \mid a$ and $d_1 \mid b$.

Consequently, $d_2 \mid a$ and $d_2 \mid b$. ...(1)

Let $x \in R$ be such that $x \mid a$ and $x \mid b$. ...(2)

Then $x \mid d_1$, since d_1 is g.c.d. of a and b.

We have $d_1 = ud_2 \Rightarrow d_2 = u^{-1} d_1 \Rightarrow d_1 \mid d_2$

Hence $x \mid d_1$ and $d_1 \mid d_2 \Rightarrow x \mid d_2$ ...(3)

From (1), (2) and (3) ; d_2 is also a g.c.d. of a and b.

Example 2.8.9. *Let R be a P.I.D. Let $d_1 \in R$ be a g.c.d. of $a, b \in R$. Show that $d_2 \in R$ is a g.c.d. of a and b if and only if d_1 and d_2 are associates.*

Solution. Refer to Examples 2.8.7, 2.8.8.

Definition. (Co-prime Elements)

Two non-zero elements of a principal ideal domain R are said to be **relatively prime** *or* **co-prime**, *if their greatest common divisor is a unit of R.*

Lemma 2.8.3. *Two elements a and b of a P.I.D. R are relatively prime iff* $(a, b) = 1$.

Proof. Let x be any unit in R. then $x\,x^{-1} = 1$, where x^{-1} is a unit in R. It follows that 1 and x are associates. Thus 1 is an associate of any unit. Since a and b are relatively prime, g.c.d. of a and b is a unit, say u *i.e.*, $u = (a, b)$. Since any associate of a g.c.d. is a g.c.d., 1 is g.c.d. of a and b. Hence $1 = (a, b)$. [See Example 2.8.8]

Conversely, $(a, b) = 1 \Rightarrow a$ and b are relatively prime, since 1 is a unit in R.

Lemma 2.8.4. *Two elements a and b of a P.I.D. R are co-prime if and only if there exist x and y in R such that* $ax + by = 1$. [D.U., 1997]

Proof. By Lemma 2.8.3 ; a and b are co-prime $\Rightarrow 1 = (a, b)$.

By Theorem 2.8.2, there exist $x, y \in R$ such that $ax + by = 1$.

Conversely, let $ax + by = 1$, for some $x, y \in R$.

Let $d \in R$ be a g.c.d of a and b. Then $d \mid a$ and $d \mid b$

$\Rightarrow d \mid ax$ and $d \mid by$,

$\Rightarrow d \mid (ax + by) \Rightarrow d \mid 1 \Rightarrow d \mid 1 \Rightarrow d$ is a unit. Hence a and b are co-prime.

Lemma 2.8.5. *Let R be a principal ideal domain and* $a, b, c \in R$. *If* $a \mid bc$ *and* $(a, b) = 1$, *then* $a \mid c$.

Proof. Since $(a, b) = 1$, there exist $x, y \in R$ such that $ax + by = 1$ (Theorem 2.8.2). It follows that $cax + cby = c \cdot 1$ or $acx + bcy = c$.

Now $a \mid a \Rightarrow a \mid acx$ and $a \mid bc \Rightarrow a \mid bcy$.

$\therefore \quad a \mid (acx + bcy) \Rightarrow a \mid c$.

Theorem 2.8.6. *Prove that any two non-zero elements a and b in a P.I.D. R have a l.c.m.*

Proof. Let $A = (a)$ and $B = (b)$ be two ideals of R generated by a and b, respectively. It follows that $A \cap B$ is an ideal of R. Since R is a P.I.D., $A \cap B$ must be a principal ideal *i.e.*,

$$A \cap B = (l), \text{ for some } l \in A \cap B.$$

We shall show that l is l.c.m. of a and b.

$$l \in A \cap B \Rightarrow l \in A = (a) \text{ and } l \in B = (b)$$

$\Rightarrow l = ax$ and $l = by$, for some $x, y \in R$

$\Rightarrow a \mid l$ and $b \mid l$. ...(1)

Let $x \in R$ be such that $a \mid x$ and $b \mid x$. ...(2)

Then $x = ar$ and $x = bs$, for some $r, s \in R$

$\Rightarrow \quad x \in A = (a)$ and $x \in B = (b)$

$\Rightarrow \quad x \in A \cap B = (l) \Rightarrow x = lt$, for some $t \in R$

$\Rightarrow \quad l \mid x$. ...(3)

From (1), (2), (3) ; it follows that l is l.c.m. of a and b.

Theorem 2.8.7. *Prove that if R is a P.I.D. and a, b are two non-zer elements of R, then* $[a, b]\,(a, b) = abu$, *for some unit* $u \in R$.

Solution. Since R is a P.I.D., a and b possess g.c.d. and l.c.m.

We suppose that

$$d = (a, b) = \text{g.c.d. of } a \text{ and } b,$$
$$l = [a, b] = \text{l.c.m. of } a \text{ and } b.$$

By definition of l.c.m., $a \mid l$ and $b \mid l$ ...(1)

$\Rightarrow \quad l = ax,\ l = by$, for some $x, y \in R$.

Since d is g.c.d. of a and b, there exist λ and $\mu \in R$ such that

$$d = \lambda a + \mu b \Rightarrow l(\lambda a + \mu b) = ld$$
$$\Rightarrow \quad ld = l\lambda a + \lambda\mu b \Rightarrow ld = by\lambda a + ax\mu b$$
$$\Rightarrow \quad ld = ab(\mu x + \lambda y) \Rightarrow ab \mid ld. \qquad ...(2)$$

By definition of g.c.d., $d \mid a$ and $d \mid b$

$$\Rightarrow \quad a = dr \text{ and } b = ds, \text{ for some } r, s \in R$$
$$\Rightarrow \quad ab = drds = (drs)\,d. \qquad ...(3)$$

Now $a = dr$ and $dr \mid drs \Rightarrow a \mid drs$, $b = ds$ and $ds \mid drs \Rightarrow b \mid drs$.

$\therefore \quad a \mid drs$ and $b \mid drs$ ...(4)

From (1) and (4), $l \mid drs$ and so $drs = lt$, for some $t \in R$.

Putting in (3) gives $ab = ltd = (ld)\,t \Rightarrow ld \mid ab.$ ...(5)

From (2) and (5), ab and ld are associates. [See Example 2.7.4]

Consequently, $ld = uab$, for some unit $u \in R$.

Hence $[a, b]\,(a, b) = abu$, for some unit $u \in R$.

Example 2.8.10. *Let R be a P.I.D. Let* $l_1 \in R$ *be l.c.m. of* $a, b \in R$. *Show that* $l_2 \in R$ *is l.c.m. of a and b if and only if* l_1 *and* l_2 *are associates.*

Solution. By Theorem 2.8.6, any two non-zero elements a and b in R have a l.c.m. Let l_1 and l_2 be two least common multiples of a and b. Then $a \mid l_1$ and $b \mid l_1$; $a \mid l_2$ and $b \mid l_2$. Since l_1 is l.c.m. of a and b, so $a \mid l_2$ and $b \mid l_2 \Rightarrow l_1 \mid l_2$. Since l_2 is l.c.m. of a and b, so $a \mid l_1$ and $b \mid l_1 \Rightarrow l_2 \mid l_1$.

Hence $l_1 \mid l_2$ and $l_2 \mid l_1 \Rightarrow l_1$ and l_2 are associates.

Conversely, let l_1 be l.c.m. of a and b and l_2 be an associate of l_1.

We shall prove that l_2 is l.c.m. of a and b.

Since l_1 and l_2 are associates, $l_2 = ul_1$, for some unit $u \in R$

$\Rightarrow \quad l_1 \mid l_2$, where $a \mid l_1$ and $b \mid l_1$

$\Rightarrow \quad a \mid l_2$ and $b \mid l_2$. ...(1)

Let $x \in R$ be such that $a \mid x$ and $b \mid x$. ...(2)

Since l_1 is l.c.m. of a and b, so $a \mid x$ and $b \mid x \Rightarrow l_1 \mid x$.

Since u is a unit in R, so $l_2 = ul_1 \Rightarrow l_1 = u^{-1} l_2 \Rightarrow l_2 \mid l_1$.

Now $l_2 \mid l_1$ and $l_1 \mid x \Rightarrow l_2 \mid x$. ...(3)

From (1), (2) and (3) ; l_2 is l.c.m. of a and b.

→ In an Euclidean ring R each pair of non-zero elements a, b have a greatest common divisor. Further if $d = (a, b)$ then $d = \lambda a + \mu b$ for some $\lambda, \mu \in R$.

Soln: Let $U = \{ ra + sb / r, s \in R \}$

For $r = 1, s = 0 \in R$, $ra + sb = a \in U$.

$\therefore U$ is a non-empty subset of R.

Let $x, y \in U$ and $t \in R$.

Then $x = r_1 a + s_1 b$, $y = r_2 a + s_2 b$

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

$$x - y = (r_1 - r_2) a + (s_1 - s_2) b$$
$$= r' a + s' b$$
where $r' = r_1 - r_2$, $s' = s_1 - s_2 \in R$.

$$tx = t(r_1 a + s_1 b) = (t r_1) a + (t s_1) b$$
$$= r'' a + s'' b$$
where $r'' = t r_1$, $s'' = t s_1 \in R$.

$\therefore x, y \in U, t \in R \Rightarrow x - y \in U$ and $tx \in U$

$\therefore U$ is an ideal of R.

Since R is a principal ideal ring,

U is a principal ideal.

$\therefore$ there exists $d \in R$, such that $U = (d)$.

Then every element of U is of the form dq where $q \in R$.

Since $U = \{ ra + sb / r, s \in R \}$,

$ra + sb = dq \quad \forall r, s \in R$

$\therefore d/ra+sb \quad \forall r, s \in R$

for $r=1, s=0$, we see that d/a and

for $r=0, s=1$, we see that d/b.

Hence, if c/a, c/b then $c/ra+sb \quad \forall r, s \in R$.

i.e., c/d as $d \in U$.

$\therefore$ d is a greatest common divisor of a and b.

Since $d \in U$ there exist $\lambda, \mu \in R$ such that

$$d = \lambda a + \mu b.$$

→ If a, b, c are elements of an Euclidean ring R and a/bc; a, b are relatively prime, then a/c.

Soln: Given that a, b are relatively prime $\Rightarrow (a,b)=1$.

By the above theorem there exist $\lambda, \mu \in R$

such that $a\lambda + b\mu = 1$.

$\Rightarrow c(a\lambda + b\mu) = c \cdot 1$

$\Rightarrow (ca)\lambda + (cb)\mu = c$

$\Rightarrow (ca)\lambda + (aq)\mu = c \quad (\because a/bc \Rightarrow bc = aq$ for some $q \in R)$

$\Rightarrow a(c\lambda + q\mu) = c$

$\Rightarrow ad = c$ where $d = c\lambda + q\mu \in R$

$\Rightarrow a/c$.

→ Every non-zero element in an Euclidean ring R is either a unit in R or can be written as the product of a finite number of prime elements in R.

Soln: Let $a \in R$ and $a \neq 0$.

Case(1): Let $a \in R$ be a unit.

Then the theorem is true.

Case(2): Let $a \in R$ be not a unit and $d(a) = 0$

Suppose that $a = bc$ where c is not a unit.

Since c is not a unit, $d(bc) > d(b)$.

i.e., $d(a) > d(b) \Rightarrow d(b) < 0$.

This is impossible.

$\therefore$ c is unit and hence 'a' is a prime element.

Case (3): We apply the method of induction on $d(a)$

Suppose that the theorem is true for all $x \in R$ such that $d(x) < d(a)$,

If $a \in R$ is a prime element there is nothing to prove.

If $a \in R$ is not a prime, then $a = bc$ where neither b nor c is a unit in R.

By known theorem

$d(b) < d(bc)$, $d(c) < d(bc)$

[$\because$ Let a, b be two non-zero elements of an Euclidean ring R. Then if b is not a unit in R, $d(a) < d(ab)$]

Since $a = bc$

$\therefore$ $d(b) < d(a)$ and $d(c) < d(a)$

So, by our induction hypothesis, b and c can be written as a product of finite number of prime elements of R.

Let $b = p_1 p_2 \cdots p_r$ and $c = q_1 q_2 \cdots q_s$

where p's and q's are prime elements of R.

$\therefore$ $a = bc = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s$

= product of finite number of elements of R.

Thus if the theorem is true for $x \in R$ such that $d(x) < d(a)$ then the theorem is true for 'a'.

$\therefore$ By induction the theorem is true for all elements of R.

→ In a principal Ideal Domain an element is prime iff it is irreducible.

Sol^n: Let R be a PID. Since R is an ID., by known theorem (i.e, Let R be an ID with unity then every prime element of R is irreducible) every element of R is irreducible.

Now we shall show that every irreducible element of R is prime.

Let p be any irreducible element of R. Then $p \neq 0$ and p is not a unit.

We shall show that p is prime.

Let p/ab where $a, b \in R$.

Let $p \nmid a$ we shall show that p/b.

Since $\langle p \rangle$ and $\langle b \rangle$ are ideals of R.

So $\langle p \rangle + \langle b \rangle$ is also an ideal of R.

Since R is a PID; $\langle p \rangle + \langle b \rangle$ must be a principal ideal.

i.e., $\langle p \rangle + \langle b \rangle = \langle d \rangle$, for some $d \in R$. ——— (1)

From (1), $\langle p \rangle \subset \langle d \rangle$

$\Rightarrow p \in \langle d \rangle$

$\Rightarrow p = dx$, for some $x \in R$. ——— (2)

Since p is irreducible., either d or x is a unit. Suppose d is a unit

Then $\bar{d} \in R$ and $d\bar{d} = 1$

$\Rightarrow 1 \in \langle d \rangle$

$\Rightarrow 1 \in \langle p \rangle + \langle d \rangle$, by (1)

$\Rightarrow 1 = pr+bs$, for some $r, s \in R$

$\Rightarrow a = a\cdot 1 = apr + abs$ ——— (3)

Now $p/p \Rightarrow p/apr$ and $p/ab \Rightarrow p/abs$

Thus $p/apr+abs$ and so p/a, by (3).

But p/a is contrary to our assumption and so d cannot be a unit. It follows that x is a unit. ie, $x^{-1} \in R$.

From (2), $d = px^{-1}$.

Let $\alpha \in \langle d \rangle$

Then $\alpha = dy$, for some $y \in R$.

$\Rightarrow \alpha = (px^{-1})y$

$= p(x^{-1}y)$, $x^{-1}y \in R$

$\Rightarrow \alpha \in \langle p \rangle \quad \forall \alpha \in \langle d \rangle$

$\Rightarrow \langle d \rangle \subseteq \langle p \rangle$.

As shown above, $\langle p \rangle \subseteq \langle d \rangle$

$\therefore \langle d \rangle = \langle p \rangle$.

Using in (1), we get

$\langle p \rangle + \langle b \rangle = \langle p \rangle$

$\Rightarrow \langle b \rangle \subseteq \langle p \rangle$

$\Rightarrow b \in \langle p \rangle$

$\Rightarrow p = pt$, for some $t \in R$

$\Rightarrow p/b$.

Hence p is prime

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

Soln: If $\mathbb{Z}[\sqrt{-5}]$ is a P.I.D; then every irreducible element of $\mathbb{Z}[\sqrt{-5}]$ must be prime.

Already we have shown that $3 \in \mathbb{Z}[\sqrt{-5}]$ is irreducible but not prime.

Hence we arrive at a contradiction and so $\mathbb{Z}[\sqrt{-5}]$ is not a PID.

→ Show that $\mathbb{Z}[\sqrt{-6}]$ is not a P.I.D.

→ Let R be a P.I.D. which is not a field. Prove that an ideal $A = \langle a \rangle$ is a maximal ideal iff a is an irreducible element of R.

Soln: Since R is not a field, there exists an element $p \neq 0 \in R$ such that p^{-1} doesnot exist i.e. p is not a unit.

condition is necessary:

Let $A = \langle a \rangle$ be a maximal ideal of R. We shall show that a is an irreducible element of R.

We observe that $a \neq 0$, for if $a = 0$, then $0 \subset \langle p \rangle \subset R$ and so $\langle a \rangle = \langle 0 \rangle$ is not a maximum ideal of R, which is a contrary to the given hypothesis.

Further, $A \neq R \Rightarrow a$ is not a unit, for if a is a unit, then $a^{-1} \in R$ and so $a \in A$ and $a^{-1} \in R \Rightarrow 1 = a a^{-1} \in A$

$\Rightarrow A = R$, which is a contradiction.

Thus $a \neq 0$ and a is not a unit.

Suppose that $a = bc$, for some $b, c \in R$.

Let $B = \langle b \rangle$. Let $r \in A = \langle a \rangle$ be arbitrary.

Then $r = ax$, for some $x \in R$ (or)

$$r = (bc)x = b(cx)$$
$$\Rightarrow r \in B$$
$$\Rightarrow A \subseteq B \subseteq R.$$

Since A is a maximal ideal of R, either $A = B$ or $B = R$.

Let $B = R$. Then $1 \in R \Rightarrow 1 \in B = \langle b \rangle$
$\Rightarrow 1 = by$, for some $y \in R$
$\therefore b/1 \Rightarrow b$ is a unit.

Let $A = B$. Then $b \in B \Rightarrow b \in A = \langle a \rangle$
$\Rightarrow b = az$, for $z \in R$
$\Rightarrow b = (bc)z$
$\Rightarrow cz = 1$
$\Rightarrow c/1$
$\Rightarrow c$ is a unit.

Hence a is an irreducible element of R.

Condition is sufficient:

Let $A = \langle a \rangle$, where a is an irreducible element of R. We shall show that A is a maximal ideal of R.

Let I be any ideal of R such that $A \subseteq I \subseteq R$.

Since R is a PID., $I = \langle d \rangle$, for some $d \in R$.

Case(1): Let $d \in A = \langle a \rangle$. Then $d = ax$ for some $x \in R$.

For any $r \in I = \langle d \rangle$, $r = dy$, for some $y \in R$.

$$\Rightarrow r = (ax)y = a(xy)$$

$$\Rightarrow r \in A$$

$$\Rightarrow I \subseteq A.$$

Also $A \subseteq I$.

$\therefore A = I$.

Case(2): Let $d \notin A$. Since $a \in A$ and $A \subseteq I = \langle d \rangle$,

so $a = dt$, for some $t \in R$.

Since R is irreducible, either d or t is a unit.

If t is a unit, then $t^{-1} \in R$ and so $d = at^{-1}$.

Since $a \in A$ and $t^{-1} \in R$, $at^{-1} \in A$, as A is an ideal of R.

Thus $d \in A$, which is a contradiction.

Consequently, d must be a unit

i.e., $d^{-1} \in R$

Now $d \in I$ and $d^{-1} \in R \Rightarrow 1 = dd^{-1} \in I$

$$\Rightarrow I = R.$$

Hence $A \subseteq I \subseteq R$

$\Rightarrow A = I$ or $I = R$

and so A is a maximal ideal of R.

Theorem 2.8.10. *Let R be a principal ideal domain. Show that any non-zero ideal $P \neq R$ is prime if and only if it is maximal.*

Proof. Let $P \neq R$ be a non-zero prime ideal of R. Since R is a P.I.D., $P = (a)$, for some $0 \neq a \in P$. We shall prove that P is a maximal ideal of R.

Let M be any ideal of R such that $P \subseteq M \subseteq R$. We can write $M = (b)$, for some $b \in M$. Since $a \in P$ and $P \subseteq M$, $a \in M \Rightarrow a = bx$, for some $x \in R$. Since P is a prime ideal of R and $a \in P$, either $b \in P$ or $x \in P$. If $b \in P$, then $(b) \subseteq P \Rightarrow M \subseteq P \Rightarrow P = M$.

If $x \in P = (a)$, then $x = ay$, for some $y \in R$. Consequently,

$$a = bx \Rightarrow a = bay \Rightarrow a \,.\, 1 = a \,.\, by \Rightarrow by = 1 \Rightarrow b \text{ is a unit.}$$

Since M is an ideal of R containing a unit b, $M = R$.

Hence P is a maximal ideal of R.

Conversely, every maximal ideal of R (being a commutative ring with unity) is a prime ideal of R. [See Theorem 2.6.3.]

Theorem 2.8.11. *Let R be a P.I.D. Show that every ascending chain of ideals*

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \ldots \subseteq (a_n) \subseteq \ldots \quad \ldots(1)$$

is finite. [D.U., 1998]

Proof. Suppose the above chain of ideals is not finite.

Let $$A = \bigcup_{i=1}^{\infty} (a_i) \,. \quad \ldots(2)$$

We proceed to show that A is an ideal of R.

Let $x, y \in A$ be arbitrary. Then, by (2), $x \in (a_m)$, $y \in (a_n)$;

for some positive integers m, n. We may assume that $m \leq n$.

Using (1), we get

$$(a_m) \subseteq (a_n) \Rightarrow x, y \in (a_n)$$

$$\Rightarrow \quad x - y \in (a_n) \Rightarrow x - y \in A, \text{ by (1).}$$

Again for any $r \in R$ and $x \in A$, we see that

$$x \in (a_m) \text{ and so } rx \in (a_m) \Rightarrow rx \in A \Rightarrow xr = rx \in A.$$

Thus A is an ideal of R and so A must be a principal ideal, as R is a P.I.D.

Let $A = (a)$, for some $a \in A$ ...(3)

Using (2), $a \in A \Rightarrow a \in (a_k)$, for some positive integer k

$$\Rightarrow \quad (a) \subseteq (a_k) \quad \Rightarrow \quad A \subseteq (a_k), \text{ by (3)}$$

$$\Rightarrow \bigcup_{i=1}^{\infty} (a_i) \subseteq (a_k), \text{ by (2)}$$

$$\Rightarrow \quad (a_i) \subseteq (a_k), \text{ for } i = 1, 2, 3, \ldots \quad \ldots(4)$$

From (1), $(a_k) \subseteq (a_{k+1}) \subseteq (a_{k+2}) \subseteq \ldots\ldots$ ...(5)

From (4), $(a_{k+1}) \subseteq (a_k)$, $(a_{k+2}) \subseteq (a_k)$ and so on. ...(6)

From (5) and (6), we obtain

$$(a_k) = (a_{k+1}) = (a_{k+2}) = \ldots$$

Hence the given ascending chain of ideals is finite *i.e.*,

$$(a_1) \subseteq (a_2) \subseteq \ldots \subseteq (a_k).$$

→ Any two non-zero elements in a Euclidean domain has a least common multiple
Hint: E.D ⇒ P.I.D.

Theorem 3.1.5. *The ideal $A = (a_0)$ is a maximal ideal of a Euclidean domain R if and only if a_0 is an irreducible (prime) element of R.*

Proof. See Theorem 2.8.9 and use the fact E.D. ⇒ P.I.D.

EXAMPLES

Example 3.1.8. *Show that* $\mathbf{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbf{Z}\}$ *is not a Euclidean domain.*

Solution. Let, if possible, $\mathbf{Z}[\sqrt{-5}]$ be a Euclidean domain. Consequently, an element in $\mathbf{Z}[\sqrt{-5}]$ is prime if and only if it is irreducible [Theorem 3.1.4]. We have seen that $3 \in \mathbf{Z}[\sqrt{-5}]$ is irreducible but not prime [See Examples 2.7.9. and 2.7.12. of chapter 2].

Hence $\mathbf{Z}[\sqrt{-5}]$ is not a Euclidean domain.

Example 3.1.9. Show that $\mathbf{Z}[\sqrt{-6}] = \{a + b\sqrt{-6} : a, b \in \mathbf{Z}\}$ *is not a Euclidean domain.*

Hint. See Example 2.7.17. $5 \in \mathbf{Z}[\sqrt{-6}]$ is irreducible but not prime.

Example 3.1.10. *In a Euclidean ring prove that any two greatest common divisors of a and b associates.* [D.U., 1995]

Hint. See Example 2.8.7, and use the fact E.D. ⇒ P.I.D.

Example 3.1.11. *State and prove a necessary and sufficient condition for an element of a Euclidean ring R to be a unit of R.* [D.U., 1999, 92]

Or

Prove that a necessary and sufficient condition that an element a in the Euclidean ring R be a unit is that $d(a) = d(1)$. [D.U., 1996]

Solution. Since R is a Euclidean domain, $1 \in R$ and by condition **(E.1)** of the definition of E.D., $d(1) \le d(1 \cdot x)\ \forall\ x \ne 0 \in R$

$$\therefore \quad d(1) \le d(x) \quad \forall\ x \ne 0 \in R. \qquad \ldots(1)$$

Condition is necessary

Let $a \in R$ be a unit in R. Then $a \mid 1$ *i.e.*, there exists some $b \in R$ such that $ab = 1$. By condition **(E.2)** of E.D.,

$$d(a) \le d(ab) \text{ or } d(a) \le d(1).$$

From (1), $d(1) \le d(a)$. Hence $d(a) = d(1)$.

Condition is sufficient

Let $d(a) = d(1)$. We shall prove that a is unit. By definition of E.D., for $1, a \in R$, there exist $t, r \in R$ such that $1 = at + r$, where either $r = 0$ or $d(r) < d(a)$.

If $r \ne 0$, then $d(r) < d(a) \Rightarrow d(r) < d(1)$, which contradicts (1).

$\therefore r = 0$ and so $1 = at \Rightarrow a \mid 1 \Rightarrow a$ is unit.

Remark. As a consequence of the above result, it follows that

The only units of $\mathbf{Z}[i]$ *are* $\pm 1, \pm i$.

Notice that $d(i) = d(-i) = d(-1) = d(1) = 1$.

$[\because\ d(a + bi) = a^2 + b^2]$

→ In a Euclidean domain, an element is prime ⇔ it is irreducible.
[Hint: E.D → P.I.D.]

Example 3.1.12. *Let a and b be two non-zero elements of a Euclidean domain R. Prove that b is not a unit in R if and only if* $d(a) < d(ab)$.

[D.U., 1993]

Proof. By condition **(E.1)** of Euclidean domain, $d(a) \leq d(ab)$. ...(1)

Consider the ideal $A = (a) = \{xa : x \in R\}$ of R.

We know $a \neq 0 \in A$ and $d(a)$ is minimal.

[See Remark 2 of Theorem 3.1.1]

Since $a \in A$ and $b \in R$, $ab \in A$ (as A is an ideal of R). Let, if possible, $d(a) = d(ab)$. By the minimality of $d(a) = d(ab)$, we conclude that $A = (ab)$. Since $a \in A$ and $A = (ab)$, $a = abx$, for some $x \in R$

$\Rightarrow a \,.\, 1 = abx \Rightarrow 1 = bx$, since $a \neq 0$ and R is an integral domain.

$\Rightarrow b \mid 1 \Rightarrow b$ is a unit in R, which is a contradiction.

$\therefore\ d(a) \neq d(ab)$ and so by (1), $d(a) < d(ab)$.

Conversely, let $d(ab) > d(a)$. We have to show that b is not a unit in R. Let, if possible, b be a unit in R. Then $b^{-1} \in R$ and $bb^{-1} = 1$.

We have $d(a) = d(a \,.\, 1) = d(a \,.\, bb^{-1}) = d(ab \,.\, b^{-1}) \geq d(ab)$, by def.

$\therefore\quad d(a) \geq d(ab)$.

Again, by definition of E.D., $d(ab) \geq d(a)$.

$\therefore\quad d(a) = d(ab)$, which is contrary to the given hypothesis.

Hence b is not a unit in R.

Example 3.1.13. *Let D be a Euclidean domain with unit element* 1. *Let x be a non-unit in D. Show that* $d(1) < d(x)$, *under usual notations. Deduce that x is a unit in D iff* $d(x) = d(1)$. [D.U., 1994]

Solution. (*i*) Since x is a non-unit in D, so $d(a) < d(ax)$, $\forall\ a \neq 0 \in D$.

[See Example 3.1.12.]

In particular, $d(1) < d(1 \,.\, x)$ (Take $a = 1 \in R$).

$\therefore\quad d(1) < d(x)$.

(*ii*) Let $d(x) = d(1)$. Then x must be a unit in D, for otherwise, $d(1) < d(x)$ [By part (*i*)], which is contrary to the given hypothesis.

Conversely, let x be a unit. Then $x \mid 1$ or $1 = xy$, for some $y \in R$. Thus $d(1) = d(xy) \geq d(x)$, by definition of E.D.

$\therefore\quad d(1) \geq d(x)$. ...(1)

Since $1 \in R$, by definition of E.D.,

$$d(1 \,.\, x) \geq d(1) \text{ } i.e., \text{ } d(x) \geq d(1). \qquad ...(2)$$

From (1) and (2), $d(x) = d(1)$.

Example 3.1.14. *Let R be a Euclidean domain and* $a, b, c \in R$. *If* $a \mid bc$ *and* $(a, b) = 1$, *prove that* $a \mid c$.

Solution. Since E.D. $\Rightarrow$ P.I.D., the result follows by Lemma 2.8.5.

Example 3.1.15. *Let R be a Euclidean domain. Prove that*

(*i*) $d(a) = d(-a)$ $\forall\ a \neq 0 \in R$.

(*ii*) *If* $d(a) = 0$ *for* $a \neq 0 \in R$, *then a is unit in R.*

Solution. (*i*) Since $1 \in R$, we see that

$a \mid -a$ and $-a \mid a \Rightarrow -a = ax$ and $a = -ay$, for some $x, y \in R$.

Now $-a = ax \Rightarrow d(-a) = d(ax) \geq d(a)$, since R is E.D.

$\therefore \quad d(-a) \geq d(a)$

Again $a = -ay \Rightarrow d(a) = d(-ay) \geq d(-a) \Rightarrow d(a) \geq d(-a)$.

Hence $d(a) = d(-a) \ \forall \ a \neq 0 \in R$.

(*ii*) For $1 \in R$, $a \neq 0 \in R$, there exist $t, r \in R$ such that

$1 = at + r$, where $r = 0$ or $d(r) < d(a)$.

If $r \neq 0$, then $d(r) < d(a)$ or $d(r) < 0$ ($\because d(a) = 0$), which is impossible, as $d(r)$ is a non-negative integer. Thus $r = 0$ and so $1 = at \Rightarrow a \mid 1 \Rightarrow a$ is unit.

Example 3.1.16. *Let a, b be two non-zero elements of a Euclidean domain R. Prove that*

(*i*) *If a and b are associates, then* $d(a) = d(b)$.

However, the converse need not be true.

Or

Show by an example that it is possible to find two elements a and b in a Euclidean domain such that $d(a) = d(b)$, *but a, b are not associates.*

[D.U., 1994]

(*ii*) *If* $a \mid b$ and $d(a) = d(b)$, *then a and b are associates.*

(*iii*) $d(a) = d(ab)$ *iff b is a unit.*

Solution. (*i*) Since a and b are associates, $a \mid b$ and $b \mid a$.

(See Example 2.7.4 of chapter 2)

Now $a \mid b \Rightarrow b = ax$, for some $x \in R$

$\Rightarrow d(b) = d(ax) \geq d(a)$, by definition of E.D.

$\Rightarrow d(a) \leq d(b)$

Similarly, $b \mid a \Rightarrow d(b) \leq d(a)$. Hence $d(a) = d(b)$.

However, the converse is not true as shown below :

We know $\mathbf{Z}[i] = \{m + ni : m, n \in \mathbf{Z}\}$ is a E.D., where

$d(m + ni) = m^2 + n^2$.

Let $a = 3 + 4i, b = 3 - 4i \in \mathbf{Z}[i]$. Then

$d(a) = d(b) = 9 + 16 = 25$.

If a and b are associates, then $a = ub$ for some unit $u \in \mathbf{Z}[i]$ *i.e.*, $u = \pm 1, \pm i$.

[We know that the units of $\mathbf{Z}[i]$ are $\pm 1, \pm i$.]

Consequently, we have

$3 + 4i = 1(3 - 4i)$ or $3 + 4i = -1(3 - 4i)$

or $3 + 4i = i(3 - 4i)$ or $3 + 4i = -i(3 - 4i)$

The above relations give us

$3 + 4i = 3 - 4i$ or $3 + 4i = -3 + 4i$

or $3 + 4i = 4 + 3i$ or $3 + 4i = -4 - 3i$.

None of these relations is possible. Hence $d(a) = d(b)$, but a and b are not associates.

(*ii*) Consider the ideal $A = (a) = \{ax : x \in R\}$ of R.

We know $a \neq 0 \in A$ and $d(a)$ is minimal.

[See Remark 2 of Theorem 3.1.1]

Since $a \mid b$, $b = ax$, for some $x \in R$.

Since $a \in A$ and A is an ideal of R, $b = ax \in A$.

Since $b \in A$ and $d(b) = d(a)$, so by the minimality of $d(a) = d(b)$, $A = (b)$. Now $a \in A \Rightarrow a \in (b) \Rightarrow a = by$, for some $y \in R \Rightarrow b \mid a$.

Hence $a \mid b$ and $b \mid a \Rightarrow a$ and b are associates.

(*iii*) Let $d(a) = d(ab)$. Then b must be a unit in R, for otherwise, $d(a) < d(ab)$ [see Example 3.1.12], which is contrary to the given hypothesis.

Conversely, let b be a unit in R.

Then $b \mid 1 \Rightarrow 1 = bc$, for some $c \in R$

$\Rightarrow a \,.\, 1 = a(bc)$, since $a \neq 0$ and R is an integral domain

$\Rightarrow a = ab \,.\, c \Rightarrow d(a) = d(ab \,.\, c) \geq d(ab)$, by def. of E.D.

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

By definition of E.D., $d(a) \leq d(ab)$. Hence $d(a) = d(ab)$.

Example 3.1.17. *If $a + bi$ is not a unit of $\mathbf{Z}[i]$, prove that $a^2 + b^2 > 1$.* [D.U., 2000, 1995, 91]

Solution. For each $a + bi \neq 0 \in \mathbf{Z}[i]$ we know

$$d(a + bi) = a^2 + b^2 \geq 1.$$

We know that the only units of $\mathbf{Z}[i]$ are $\pm 1, \pm i$ and

$$d(u) = 1 \ \forall \ u \in \{1, -1, i, -i\} \subset \mathbf{Z}[i].$$

Consequently, $d(x) > 1$ for all non-units $x \in \mathbf{Z}[i]$.

Since $a + bi$ is not a unit, $d(a + bi) > 1$.

Hence $a^2 + b^2 > 1$

Example 3.1.18. *Prove that in a Euclidean ring R, (a, b) can be found as follows :*

$$b = q_0 a + r_1, \text{ where } d(r_1) < d(a),$$
$$a = q_1 r_1 + r_2, \text{ where } d(r_2) < d(r_1)$$
$$r_1 = q_2 r_2 + r_3, \text{ where } d(r_3) < d(r_2)$$
$$\vdots \qquad\qquad \vdots$$
$$r_{n-1} = q_n r_n,$$

and $r_n = (a, b)$.

Solution. It is clear that a and b are both non-zero elements of R. By definition of E.D., there exist q_0 and $r_1 \in R$, such that

$$b = q_0 a + r_1, \text{ where either } r_1 = 0 \text{ or } d(r_1) < d(a).$$

If $r_1 \neq 0$, then $b = q_0 a + r_1$, where $d(r_1) < d(a)$.

It follows that $(a, b) = (a, r_1)$.

For $a \neq 0$, $r_1 \neq 0 \in R$, there exist $q_1, r_2 \in R$ such that

$a = q_1 r_1 + r_2$, where $d(r_2) < d(r_1)$ (of course, $r_2 \neq 0$)

It follows that $(a, b) = (a, r_1) = (r_1, r_2)$.

For $r_1 \neq 0$, $r_2 \neq 0 \in R$, there exist $q_2, r_3 \in R$ such that

$r_1 = q_2 r_2 + r_3$, where $d(r_3) < d(r_2)$.

It follows that $(a, b) = (a, r_1) = (r_1, r_2) = (r_2, r_3)$ and so on.

Proceeding in a similar manner, we shall obtain

$r_{n-1} = q_n r_n + r_{n+1}$, where $r_{n+1} = 0$.

Consequently, $r_{n-1} = q_n r_n$, where $r_n = (r_{n-1}, r_n)$.

Hence $r_n = (r_{n-1}, r_n) = \ldots = (r_1, r_2) = (a, r_1) = (a, b)$.

Remark. *The technique of this example helps us to find g.c.d. of two elements in* $\mathbf{Z}[i]$, *as explained in the following examples*

Example 3.1.19. *Let* $a = 3 + 2i$ *and* $b = 1 + 3i \in \mathbf{Z}[i]$.

Find $q, r \in \mathbf{Z}[i]$ *such that* $a = bq + r$, *where* $d(r) < d(b)$.

Solution. We have

$$\frac{a}{b} = \frac{3+2i}{1+3i} = \frac{(3+2i)(1-3i)}{(1+3i)(1-3i)} = \frac{9-7i}{10} = \frac{9}{10} - \frac{7}{10}i$$

$$= (1-i) - \frac{1}{10} + \frac{3}{10}i.$$

$$\therefore \quad a = (1-i)(1+3i) + \left(-\frac{1}{10} + \frac{3i}{10}\right)(1+3i)$$

or $$a = (1-i)(1+3i) + (-1).$$

Hence $a = bq + r$, where $q = 1 - i \in \mathbf{Z}[i]$, $r = -1 \in \mathbf{Z}[i]$ and $d(r) < d(b)$. $[\because\ d(r) = 1, d(b) = 1 + 9 = 10]$

Example 3.1.20. *If possible, find g.c.d. and l.c.m. of* $10 + 11i$ *and* $8 + i$ *in* $\mathbf{Z}[i]$. [D.U., 1998]

Solution. We have

$$\frac{10+11i}{8+i} = \frac{(10+11i)(8-i)}{(8+i)(8-i)} = \frac{91+78i}{65} = \frac{7}{5} + \frac{6}{5}i$$

or $$\frac{10+11i}{8+i} = (1+i) + \left(\frac{2}{5} + \frac{1}{5}i\right)$$

or $$10 + 11i = (1+i)(8+i) + \left(\frac{2}{5} + \frac{1}{5}i\right)(8+i)$$

or $$10 + 11i = (1+i)(8+i) + (3+2i), \text{ where } d(3+2i) < d(8+i)$$

$[\because\ d(3+2i) = 13, d(8+i) = 65]$

Now we consider

$$\frac{8+i}{3+2i}=\frac{(8+i)(3-2i)}{(3+2i)(3-2i)}=\frac{26-13i}{13}=2-i$$

or $$(8+i)=(2-i)(3+2i)$$

Hence $3+2i$ is the g.c.d. of $10+11i$ and $8+i$.

If (a, b) and $[a, b]$, respectively, denote g.c.d. and l.c.m. of a and b in $\mathbf{Z}[i]$, then

$$[a, b]=\frac{ab}{(a, b)}.$$ [See Theorem 2.8.7. Take $u=1$]

Hence l.c.m. of $a=10+11i$, $b=8+i$ is

$$=\frac{(10+11i)(8+i)}{3+2i}=\frac{(69+98i)(3-2i)}{(3+2i)(3-2i)}$$

$$=\frac{403+156i}{13}=31+12i.$$

Example 3.1.21. *Show that* $3+4i$ *and* $4-3i$ *are associates in* $\mathbf{Z}[i]$.

Solution. Clearly. $3+4i=i(4-3i)$, where i is a unit in $\mathbf{Z}[i]$.

By definition, $3+4i$ and $4-3i$ are associates.

It may be noted that g.c.d of $3+4i$ and $4-3i$ is **not** i. Indeed g.c.d. of $3+4i$ and $4-3i$ is $3+4i$ or $4-3i$ (both non-units in $\mathbf{Z}[i]$). Hence $3+4i$ and $4-3i$ **are not co-prime** in $\mathbf{Z}[i]$.

Example 3.1.22. *Find the g.c.d. in* $\mathbf{Z}[i]$ *of* 2 *and* $3+5i$.

[D.U., 1994]

Solution. We have

$$\frac{3+5i}{2}=\frac{3}{2}+\frac{5i}{2}=(1+2i)+\left(\frac{1}{2}+\frac{1}{2}i\right)$$

or $$(3+5i)=(1+2i)\,2+(1+i), \text{ where } d(1+i)<d(2).$$

Now $$\frac{2}{1+i}=\frac{2(1-i)}{(1+i)(1-i)}=\frac{2-2i}{2}=1-i$$

i.e., $$2=(1+i)(1-i).$$

Hence $1+i$ is the g.c.d. of 2 and $3+5i$.

Example 3.1.23. *Find the g.c.d. of* $11+7i$ *and* $18-i$ *in* $\mathbf{Z}[i]$.

[D.U., 2000, 1996]

Solution. We have

$$\frac{18-i}{11+7i}=\frac{(18-i)(11-7i)}{(11+7i)(11-7i)}=\frac{191-137i}{170}$$

$$=(1-i)+\left(\frac{21}{170}+\frac{33}{170}i\right).$$

$$\therefore \quad (18-i)=(1-i)(11+7i)+\left(\frac{21}{170}+\frac{33i}{170}\right)(11+7i)$$

or $$(18-i)=(1-i)(11+7i)+3i, \text{ where } d(3i)<d(11+7i).$$

Now we consider

$$\frac{11+7i}{3i}=\frac{7}{3}+\frac{11}{3i}=\frac{7}{3}-\frac{11}{3}i=(2-3i)+\left(\frac{1}{3}-\frac{2}{3}i\right)$$

or $$11+7i=(2-3i)\,3i+\left(\frac{1}{3}-\frac{2}{3}i\right)(3i)$$

or $$11+7i=(2-3i)\,3i+(2+i),\ \text{where } d(2+i)<d(3i).$$

Again $$\frac{3i}{2+i}=\frac{3i(2-i)}{(2+i)(2-i)}=\frac{3+6i}{5}=(1+2i)+\left(-\frac{2}{5}-\frac{4}{5}i\right)$$

or $$3i=(1+2i)(2+i)+\left(-\frac{2}{5}-\frac{4}{5}i\right)(2+i)$$

or $$3i=(1+2i)(2+i)-2i,\ \text{where } d(-2i)<d(2+i).$$

Further $$\frac{2+i}{-2i}=-\frac{1}{i}-\frac{1}{2}=-\frac{1}{2}+i$$

or $$2+i=i(-2i)+i,\ \text{where } d(i)<d(-2i).$$

Finally, $$-\frac{2i}{i}=-2 \text{ or } -2i=(-2)\,i.$$

Thus i is the g.c.d. of $11+7i$ and $18-i$, where i is a unit in $\mathbf{Z}[i]$. Hence $11+7i$ and $18-i$ are co-prime elements in $\mathbf{Z}[i]$.

EXERCISES

1. If $a=1+2i$ and $b=3+i\in\mathbf{Z}[i]$, find $t, r\in\mathbf{Z}[i]$ such that $a=tb+r$, where $d(r)<d(b)$. **[Ans.** $t=1, r=-2-2i$**]**
2. Find the g.c.d. of $3+2i$ and $2-3i$ in $\mathbf{Z}[i]$. **[Ans.** i**]**
3. Find the g.c.d. of $3+4i$ and $7-i$ in $\mathbf{Z}[i]$. **[Ans.** 1**]**
4. Find the g.c.d. of 3 and $4+5i$ in $\mathbf{Z}[i]$. **[Ans.** i**]**

   [Hint. Similar to Example 3.1.22**]**
5. Show that $\mathbf{Z}[\sqrt{-2}]=\{m+n\sqrt{-2}: m, n\in\mathbf{Z}\}$ is a Euclidean domain.

   [Hint. Take $d(m+n\sqrt{-2})=m^2+2n^2$.**]**
6. Let $a, b, c\in R$, R being a Euclidean domain. If $a\mid c$ and $b\mid c$ and $(a, b)=1$, prove that $ab\mid c$.

   [Hint. Let $c=ar_1, c=br_2$ and $ax+by=1$. Then

   $$c=acx+bcy=abr_2x+abr_1y=ab(r_2x+r_1y).$$ Hence $ab\mid c$. **]**
7. Let R be a Euclidean domain with valuation d. If $a, b\in R$ and $a\mid b$, then a and b are associates if and only if $d(a)=d(b)$. [D.U., 1993]

   [Hint. See Example 3.1.16 (i, ii)**]**
8. Let R be a Euclidean domain and $a, b\in R$. Prove that a is non-unit in R if and only if $d(ab)>d(b)$. [D.U., 1993]

   [Hint. See Example 3.1.12.**]**

* Polynomial Rings and Division Algorithm *

"very early in our mathematical education - in fact in junior high school or early in high school itself - we are introduced to polynomials. For a seemingly endless amount of time we are drilled, to the point of utter boredom, in factoring them, multiplying them, dividing them, simplifying them. Facility in factoring a quadratic becomes confused with genuine mathematical talent."

I. N. HERSTEIN, Topics in Algebra.

Later, at the beginning college level, polynomials make their appearance in a somewhat different setting. Now they are functions, taking on values and we become concerned with their continuity, their derivatives, their integrals, their maxima and minima.

We too shall be interested in polynomials but from neither of the above viewpoints. To us polynomials will simply be elements of a certain ring and we shall be concerned with algebraic properties of thi

Let F be a field. By the ring of polynomials in the indeterminate, x, written as F[x], we mean the set of all symbols $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, where n can

be any non-negative integer and where the coefficients $a_1, a_2, \ldots, a_n$ are all in F. In order to make a ring out of F[x], we must be able to recognize when two elements in it are equal, we must be able to add and multiply elements of F[x] so that the axioms defining a ring hold true for F[x].

Note: we could avoid the phrase "the set of all symbols" used above by introducing an appropriate apparatus of sequences but it seems more desirable to follow a path which is some what familiar to most readers.

Polynomial: Let R be a ring. Let $x \notin R$ where x is indeterminate. The expression of the form

$$f(x) = a_0x^0 + a_1x^1 + a_2x^2 + \cdots + a_nx^n. \quad \forall a_i \in R.$$

and n is a non-negative integer is called a polynomial in x over R. Here a_ix^i are called the terms of the polynomial and a_i are called the coefficients of the terms of the polynomial.

→ If n is the largest non-negative integer such that $a_n \neq 0$ then 'a_n' is called the leading coefficient.

Ex-①:

$$5x^0 - 7x^2 - 8x^4 - \frac{3}{2}x^5.$$

This is called a polynomial in x. Since the coefficients are rationals.

∴ It is a polynomial in 'x' over the field of rationals.

Ex:(2): $5x^2 + \pi x^2 + 7x^4$.

This is polynomial over the field of reals.

Equal polynomials:

→ Let $f(x) = a_0x^0 + a_1x^1 + \cdots + a_ix^i + \cdots + a_mx^m$ and $g(x) = b_0x^0 + b_1x^1 + \cdots + b_ix^i + \cdots + b_nx^n$ be two polynomials over R.

$f(x) = g(x)$ iff the coefficients of x are same on both sides except zero coefficients.

i.e., $f(x) = g(x)$ iff $a_i = b_i \ \forall i \geq 0$ except zero coefficient.

Ex: $5x^0 + 7x^2 + 9x^7$ is a polynomial over integers.

∴ It is a polynomial in x over the ring of integers.

Again $5x^0 + 0x^1 + 0x^2 + 7x^3 + 0x^4 + 0x^5 + 0x^6 + 9x^7$ ——— (1)

These polynomials are equal.

(∵ Coefficients of like powers of x on both sides are equal).

→ **Monic polynomial**: A polynomial is called monic polynomial when the leading coefficient is the unity element.

→ **Ring of polynomials:**

Let R be a ring. The ring of polynomials in the indeterminate 'x' denoted as R[x], is defined as the set.

$$R[x] = \left\{ f(x) = a_0x^0 + a_1x^1 + a_2x^2 + \cdots + a_nx^n \;/\; a_i \in R \text{ and } n \geq 0 \in \mathbb{Z} \right\}.$$

We shall give $R[x]$ a ring structure as follows:

Let $f(x) = a_0x^0 + a_1x^1 + \cdots + a_nx^n \in R[x]$

$g(x) = b_0x^0 + b_1x^1 + \cdots + b_mx^m \in R[x]$

we define:

Sum: $f(x) + g(x) = (a_0+b_0)x^0 + (a_1+b_1)x^1 + \cdots + (a_i+b_i)x^i + \cdots$

$= c_0 + c_1x + c_2x^2 + \cdots + c_ix^i + \cdots$ ——— (A)

Product:

$f(x)\,g(x) = c_0 + c_1x + c_2x^2 + \cdots + c_ix^i + \cdots$ ——— (B)

where $c_0 = a_0b_0$, $c_1 = a_0b_1 + a_1b_0$, $c_2 = a_0b_2 + a_1b_1 + a_2b_0$

$c_i = a_0b_i + a_1b_{i-1} + a_2b_{i-2} + \cdots + a_{i-1}b_1 + a_ib_0$

→ It is easy to verify that $R[x]$ is a ring w.r.t the compositions given by (A) and (B), where the additive identity is $0 = 0 + 0\cdot x + 0x^2 + \cdots$ and the additive inverse of $f(x)$ is $-f(x) = -a_0 - a_1x - a_2x^2 - \cdots - a_nx^n$.

— The ring $R[x]$ is also called the ring of polynomials over R and the elements of $R[x]$ are called polynomials over R.

— It is easy to verify that

(i) If R is commutative then $R[x]$ is also commutative.

(ii) If R has unity 1 then $R[x]$ also has unity where $1 = 1 + 0x + 0x^2 + \cdots$

(iii) If F is a field then $F[x]$ is commutative ring with unity. However $F[x]$ is not a field.

Ex: $f(x) = 1 \cdot x \in F[x]$ (i.e., $f(x) = a_0 + a_1 x$ where $a_0 = 0$) has no multiplicative inverse in $F[x]$.

Since if $g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m \in F[x]$ & the multiplicative inverse of $f(x)$ then $f(x) \cdot g(x) = 1$

i.e, $c_0 + c_1 x + c_2 x^2 + \cdots = 1 + 0x + 0x^2 + \cdots$

$\Rightarrow c_0 = 1, c_1 = 0, c_2 = 0, \cdots$

$\Rightarrow a_0 b_0 = 1$

$\Rightarrow 0 \cdot b_0 = 1$

$\Rightarrow 0 = 1$

which is a contradiction.

→ If R is an ID then $R[x]$ is an Integral Domain.

Soln: Since R is commutative

$\Rightarrow R[x]$ is a commutative ring.

Now $R[x]$ has no zero divisors.

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

where $f(x) = a_0 + a_1 x + \cdots + a_n x^n$

$g(x) = b_0 + b_1 x + \cdots + b_m x^m$.

$a_n \neq 0$, $b_m \neq 0 \in R$.

Then $f(x) \cdot g(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n+m} x^{n+m}$

where $c_{n+m} = a_n b_m \neq 0$

(Since R is an ID)

$\therefore f(x) g(x) \neq 0 \in R[x]$

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

→ If F is a field then F[x] is an ID.

Soln: Since F is a field.

⇒ F is an ID

∴ F[x] is an ID.

Degree of a polynomial:

Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$

we say that f(x) is a non-zero polynomial, if atleast one of the coefficients $a_0, a_1, a_2, \ldots$ is not zero.

we say that f(x) has degree 'n' if $a_n \neq 0$.

we write it as $\deg(f(x)) = n$

(or) $\deg f = n$

i.e, the highest power of x in the polynomial is called its degree.

Note: (1) The degree of polynomial non-negative.

(2) The degree of zero polynomial is undefined.

i.e, the polynomial $0x^0 + 0x^1 + 0x^2 + \cdots$ has no degree.

(3) The degree of a constant polynomial is zero.

i.e, the polynomial $a_0 x^0$ $(a_0 \neq 0)$ has degree zero.

Ex:

→ Let $f(x) = 2 + 3x + 5x^2$ and $g(x) = 3 - 5x + x^3$ be two polynomials over the ring of integers.

$\deg f = 2$, $\deg g = 3$.

we have $f(x) + g(x) = 5 - 2x + 5x^2 + x^3$ and

$f(x)\,g(x) = 6 - x - 23x^3 + 3x^4 + 5x^5.$

$\therefore \deg(f+g) = 3$ and $\deg(fg) = 5.$

→ Let $f(x)$ and $g(x)$ be two non-zero polynomials in $R[x]$ of degree m and n respectively, R being any ring.

Then (i) $\deg(f(x)+g(x)) = \max(m,n)$ when $m \neq n$

(ii) $\deg(f(x)+g(x)) \leq m$ when $m = n$

provided $f(x)+g(x)$ is not a zero polynomial.

Ex-①: Let $f(x) = 1+x+x^2$ and $g(x) = 2+3x+x^2$ be two polynomials over the ring of integers.

$\deg f = 2$, $\deg g = 2$

and $\deg(f+g) = 2$

$\deg(f+g) = 2 = \deg f$ (or) $\deg g$

Ex-②: Let $f(x) = 1+x+x^2$, $g(x) = 2+3x-x^2$.

then $f+g = 3+4x$

Now $\deg(f+g) = 1.$

$\therefore \deg(f+g) = 1 \leq \deg f$ (or) $\deg g$

→ If $f(x)$ & $g(x)$ are two non-zero polynomial elements of $F[x]$ and if $f(x)\cdot g(x) \neq 0.$

then $\deg(f(x)\cdot g(x)) \leq \deg f(x) + \deg g(x).$

Ex: Let $Z_4[x]$ be the ring of polynomials over the ring Z_4 of integers where $Z_4 = \{0, 1, 2, 3\}$

(i) Let $f(x) = x^2 + 2x + 3$ and $g(x) = 3x^2 + 2x$

then $f(x) + g(x) = (1+3)x^2 + (2+2)x + (3+0)$

$= 0x^2 + 0x + 3 = 3.$

$(\because 2+2 \equiv 0 \pmod 4$

$1+3 \equiv 0 \pmod 4)$

and $f(x) \cdot g(x) = (1\cdot 3)x^4 + (1\cdot 2 + 2\cdot 3)x^3 + (2\cdot 2 + 3\cdot 3)x^2 + 2x$

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

Now $\deg f = 2$, $\deg g = 2$

$\deg(f+g) = 0$ and $\deg(fg) = 4$

$\therefore \deg(f+g) \leq \max(2,2)$

and $\deg(fg) = 4 = \deg f + \deg g.$

(ii) Let $f(x) = 2x^2 + 2x + 3$ & $g(x) = 2x^2 + 2x.$

then $f(x) + g(x) = (2+2)x^2 + (2+2)x + 3$

$= 0x^2 + 0x + 3$

$= 3$

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

$= 0x^4 + 0x^3 + 0x^2 + 0x^2 + 2x^2 + 2x$

$= 2x^2 + 2x$

Now $\deg f = 2$, $\deg g = 2$

$\deg(f+g) = 0$ and $\deg(f\cdot g) = 2$

$\therefore \deg(f+g) \leq \max(2,2).$

and $\deg(fg) = 2 \leq \deg f + \deg g.$

→ If R is an ID then $\deg(fg) = \deg f + \deg g$

→ If R is an ID then $\deg f \leq \deg(fg)$

→ If $f(x), g(x)$ are two non-zero polynomials of $F[x]$ where F is a field then $\deg(fg) = \deg f + \deg g.$

→ Let $f(x)$ and $g(x)$ be two non-zero polynomials in $R[x]$, R being any ring.

(i) If $f(x)+g(x) \neq 0$ then $\deg(f(x)+g(x)) \leq \max(\deg f(x), \deg g(x))$

(ii) If $f(x)\cdot g(x) \neq 0$, then $\deg(f(x)\cdot g(x)) \leq \deg f(x) + \deg g(x)$.

(iii) If R is an integral domain, then

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

Sol Let $R[x]$ be the ring of polynomials of a ring R. Let $f(x)$ and $g(x)$ be two non-zero poly. in $R[x]$ s.t $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m \in R[x]$; $a_m \neq 0$ in R.

and $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n \in R[x]$; $b_n \neq 0$ in R.

Then we have $\deg f(x) = m$ & $\deg g(x) = n$.

Further $a_i = 0$ for $i > m$ and $b_j = 0$ for $j > n$.

(i) we have $f(x)+g(x) = (a_0+b_0) + (a_1+b_1)x + (a_2+b_2)x^2 + \cdots + (a_t+b_t)x^t$

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

Now $a_k + b_k = 0$ $\forall$ $k > t$ as $a_k = 0$, $b_k = 0$.

$\therefore \deg(f(x)+g(x)) \leq t \ (= \max(m,n))$.

Note: it is possible to have $\deg(f(x)+g(x)) < \max(m,n)$

for example: Let us consider the ring $\mathbb{Z}$ of integers.

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

$g(x) = 2+3x+2x^2$ be two poly. in $\mathbb{Z}[x]$.

then $f(x)+g(x) = 3+5x$.

$\therefore \deg(f(x)+g(x)) = 1$ where as
$\deg(f(x)) = 2 = \deg(g(x))$.

(ii) Let $f(x)\cdot g(x) = a_0b_0 + (a_0b_2 + a_1b_1 + a_2b_0)x + \cdots$
$\cdots + (a_0b_i + a_1b_{i-1} + a_2b_{i-2} + \cdots + a_ib_0)x^i + \cdots$
$= c_0 + c_1x + c_2x^2 + \cdots + c_ix^i + \cdots$

where $c_i = a_0b_i + a_1b_{i-1} + \cdots + a_ib_0$.

Here $c_{m+n} = a_0b_{m+n} + a_1b_{m+n-1} + \cdots + a_mb_n + \cdots + a_{m+n}b_0$.

$= a_mb_n$ as all other terms are equal to zero.

(i.e $a_{m+i} = 0$, $b_{n+j} = 0$ for all $i, j > 0$)

Again $c_{m+n+t} = 0 \quad \forall t > 0$.

Thus $\deg(f(x)\cdot g(x)) \le m+n$ ($a_mb_n = 0$ even if $a_m \neq 0, b_n \neq 0$)

Note(1): It is possible to have $\deg(f(x)\cdot g(x)) < m+n$.

for example:

Let us consider the ring $Z_6 = \{0,1,2,3,4,5\}$ of integers under modulo 6.

Let $f(x) = 1+2x^3$
$g(x) = 2+x+3x^2$ be two elts in $Z_6[x]$.
of degree 3 and 2 respectively.

Here $f(x)\cdot g(x) = 2+x+3x^2+4x^3+2x^4$.
clearly which is of degree $4 < 5$. (i.e $3+2 = 5$)

Note(2) Here R is not ID.

(iii) If R is an ID then as $a_m \neq 0$, $b_n \neq 0$

Therefore, $a_m \cdot b_n \neq 0$

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

This shows that

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

→ If $f(x)$, $g(x)$ are two non-zero polynomials in $F[x]$ (F being a field), then

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

Soln. Since every field is an integral domain, the result follows by above part (iii)

→ If $f(x)$, $g(x)$ are two non-zero polynomials in $F[x]$ (F being a field), then

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

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

Soln: we have

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

$$\geq \deg f(x), \text{ since } \deg g(x) \geq 0$$

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

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

→ If R is an integral domain with unity, then the units of R and $R[x]$ are same.

Sol^n: Let a_0 be a unit of R. Then a_0 divides 1

i.e, $a_0 / 1$

i.e, there exists some $b_0 \in R$ such that

$a_0 b_0 = 1$.

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

$g(x) = b_0 + 0x + 0x^2 + \cdots$

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

$f(x)\, g(x) = a_0 b_0 + 0x + 0x^2 + \cdots$

(or) $f(x)\, g(x) = 1 \quad (\because a_0 b_0 = 1)$

$\Rightarrow f(x) / 1$ (i.e, $f(x)$ divides 1) in $R[x]$

$\Rightarrow f(x)$ is a unit in $R[x]$.

Hence $a_0 = f(x)$ is a unit in $R[x]$.

Conversely, let $f(x)$ be a unit of $R[x]$.

Then there exists some $g(x) \in R[x]$ such that

$f(x)\, g(x) = 1 = 1 + 0x + 0x^2 + \cdots$ ——— (1)

$\Rightarrow \deg\big(f(x)\, g(x)\big) = \underset{=0}{\deg(1 + 0x + 0x^2 + \cdots)}$

$\Rightarrow \deg f(x) + \deg g(x) = 0 \quad (\because R$ is ID, $\deg(f(x)\, g(x)) = \deg f(x) + \deg g(x))$

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

$\Rightarrow f(x)$ and $g(x)$ are constant polynomials,

say $f(x) = \alpha \ (\alpha \neq 0 \in R)$, $g(x) = \beta \ (\beta \neq 0 \in R)$

$\Rightarrow \alpha\beta = 1$ by (1)

$\Rightarrow \alpha / 1$ (i.e, α divides 1) in R

Hence $f(x) = \alpha$ is a unit of R.

Problems:

→ Find the sum and product of $f(x) = 5+4x+2x^2+2x^3$ and $g(x) = 1+4x+5x+x^3$ over $(Z_6, +_6, \times_6)$.

→ $f(x) = \bar{1}+\bar{2}x$ and $g(x) = \bar{5}+\bar{4}x+\bar{3}x^2$ over $Z_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$. Prove that $\deg(f(x), g(x)) \neq \deg f(x) + \deg g(x)$

Soln: $\deg f(x) = 1$; $\deg g(x) = 2$

$\Rightarrow \deg f(x) + \deg g(x) = 1+2 = 3$

Now $f(x).g(x) = (\bar{1}\times\bar{5}) + (\bar{1}\times\bar{4}+\bar{2}\times\bar{5})x + (\bar{1}\times\bar{3}+\bar{2}\times\bar{4})x^2 + (\bar{2}\times\bar{3})x^3$

$= \bar{5}+\bar{14}x+\bar{11}x^2+\bar{6}x^3$

$= \bar{5}+\bar{2}x+\bar{5}x^2+\bar{0}x^3$

$= \bar{5}+\bar{2}x+\bar{5}x^2$

$\therefore \deg(f(x).g(x)) = 2$

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

→ Find the sum and product of the following polynomials

(i) $f(x) = 4x-5$, $g(x) = 2x^2-4x+2$ in $Z_8[x]$

(ii) $f(x) = 1+3x$, $g(x) = 4+5x+2x^3$ in $Z_6[x]$

(iii) $f(x) = 7+9x+5x^2+11x^3-2x^4$, $g(x) = 3-2x+7x^2+8x^3$ over the ring of integers

(iv) $f(x) = 2x^3+4x^2+3x+2$, $g(x) = 3x^4+2x+4$ over the ring $Z_5 = \{0,1,2,3,4\}$ of mod 5.

(v) $f(x) = 4x^3+2x^2+x+3$, $g(x) = 3x^4+3x^3+3x^2+x+4$ in $Z_5[x]$.

→ over the ring $Z_7 = \{0,1,2,3,4,5,6\}$ modulo 7, if $f(x) = 7+9x+5x^2+11x^3-2x^4$, $g(x) = 3-2x+7x^2+8x^3$.

P.T. $\deg(f(x)+g(x)) = 4$ and $\deg(f(x).g(x)) = 4$.

→ Let $f(x) = 2x^4 + 3x^3 + 2$ and $g(x) = 3x^5 + 4x^3 + 2x + 3$ be two polynomials over the field $Z_5 = (\{0,1,2,3,4\}, +_5, \times_5)$. Determine (i) $\frac{d}{dx} f(x)$ (ii) $f(x) \cdot g(x)$

→ If $f(x) = 3x^7 + 2x + 3$, $g(x) = 5x^3 + 2x + 6$ be two polynomials over the field $Z_7 = (\{0,1,2,3,4,5,6\}, +_7, \times_7)$ Determine (i) $\frac{d}{dx} f(x)$ (ii) $f(x) \cdot g(x)$ (iii) $f(x) + g(x)$.

→ If R is an I.D with unity, then any irreducible elt of R is an irreducible elt of $R[x]$.

Sol Let a be any irreducible elt of R then we have to p.T a is also an irreducible elt of $R[x]$.

If possible let a be not an irreducible elt of $R[x]$.

Then we have

$a = f(x) \cdot g(x)$, where $f(x), g(x) \in R[x]$. ①

and $f(x), g(x)$ are both non-unit fns $R[x]$.

W.K.T the units of R and $R[x]$ are the same.

$\therefore f(x)$ & $g(x)$ can not be fn R.

Let $f(x) \notin R$, from ①, we have

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

($\because$ R is I D)

$\Rightarrow 0 = \deg f(x) + \deg g(x)$ ($\because a \in R \Rightarrow \deg a = 0$)

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

If $\deg f(x) = 0$ then $f(x)$ is a constant

polynomial of the form $f(x) = \alpha$
where $\alpha \neq 0 \in R$.
$\Rightarrow f(x) \notin R$ which is a contradiction.
Hence a is an irreducible elt in $R[x]$.

→ Show that every ring R can be imbedded in the polynomial ring $R[x]$.
(or)
S.T every ring R isomorphic to a subring of $R[x]$.

Sol Define a mapping $\theta : R \longrightarrow R[x]$ as
$\theta(a) = a + 0x + 0x^2 + \cdots \quad \forall a \in R$.
It is clear that θ is 1–1
because for any $a, b \in R$
we have $\theta(a) = \theta(b)$
$\Rightarrow a + 0x + 0x^2 + \cdots = b + 0x + 0x^2 + \cdots$.
$\Rightarrow a = b$.
Now we show that
θ is a homomorphism, we have
$\theta(a+b) = (a+b) + 0x + 0x^2 + \cdots$
$= (a + 0x + 0x^2 + \cdots) + (b + 0x + 0x^2 + \cdots)$
$= \theta(a) + \theta(b)$
&
$\theta(ab) = ab + 0x + 0x^2 + \cdots$
$= (a + 0x + 0x^2 + \cdots)(b + 0x + 0x^2 + \cdots)$
$= \theta(a)\,\theta(b)$.
$\therefore$ Hence θ is an isomorphism of R into $R[x]$ i.e R is imbedded in $R[x]$.

Note :- $\phi : R \to \phi(R)$ is an onto isomorphism when $\phi(R)$ is a subring of $R[x]$ Hence R is isomorphic to a subring of $R[x]$.

→ S.T a ring R is an I.D $\iff$ $R[x]$ is an I.D.

Sol : R is an I.D. $\Rightarrow$ $R[x]$ is an I.D (It can be easily proved).

conversely, let $R[x]$ be an I.D.

W.K.T $R \cong \phi(R)$, where $\phi(R)$ is a subring of $R[x]$.

$\Rightarrow \phi(R) \cong R$

since the subring of an I.D is an I.D

$\therefore \phi(R)$ is an I.D.

since the isomorphic image of an I.D is an I.D.

$\therefore \phi(R) \cong R \Rightarrow R$ is I.D.

→ If a ring R has no proper zero divisors, then prove that $R[x]$ has no proper zero divisors.

Sol let $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \neq 0$ in $R[x]$, $a_n \neq 0 \in R$.

and $g(x) = b_0 + b_1x + \cdots + b_mx^m \neq 0$ in $R[x]$

$b_m \neq 0 \in R$.

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

and

$a_i = 0$ for each $i \geq n+1$

&

$b_j = 0$ for each $j \geq m+1$. ——— (1)

we have

$f(x) \cdot g(x) = c_0 + c_1x + c_2x^2 + \cdots$

where $c_{n+m} = a_0 b_{n+m} + a_1 b_{n+m-1} + \cdots$

$\cdots + a_{n-1} b_{m+1} + a_n b_m$.

$+ \cdots + a_{n+1} b_{m+1} + \cdots + a_{n+m} b_0$.

$= a_n b_m$ by (1)

$\therefore c_{n+m} = a_n b_m$

$\neq 0$ ($\because$ R has no proper zero divisors).

Hence $f(x)g(x) \neq 0$ and so

$R[x]$ has no proper zero divisors.

exercises

→ Let R be a commutative ring with no non-zero nilpotent elements. If $f(x) = a_0 + a_1x + \cdots + a_mx^m$ in $R[x]$ is a zero divisor, Prove that there is an element $b \neq 0$ in R such that

$$ba_0 = ba_1 = \cdots = ba_m = 0.$$

Sol^n: Since R has no non-zero nilpotent elements, so for all positive integers n, $a^n = 0 \Rightarrow a = 0 \;\forall\, a \in R$.

Since $f(x) \in R[x]$ is a zero divisor, there exists some $g(x) \in R[x]$ such that

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

Let $g(x) = b_0 + b_1x + \cdots + b_nx^n \in R[x]$.

we may suppose that $a_m \neq 0$ and $b_n \neq 0 \in R$. we have

$$(a_0 + a_1x + \cdots + a_{m-1}x^{m-1} + a_mx^m)(b_0 + b_1x + \cdots + b_{n-1}x^{n-1} + b_nx^n) = 0 + 0x + 0x^2 + \cdots$$

It follows that

$a_mb_n = 0$, $a_{m-1}b_n + a_mb_{n-1} = 0, \ldots, a_0b_1 + a_1b_0 = 0$, $a_0b_0 = 0$

we have $(a_{m-1}b_n + a_mb_{n-1}) = 0$, $b_n = 0$.

(or) $a_{m-1}b_n^2 = 0$ since R is commutative and $a_mb_n = 0$

Similarly, $a_{m-2}b_n^3 = 0, \ldots, a_1b_n^m = 0$ and $a_0b_n^{m+1} = 0$

Let $b = b_n^{m+1}$. Then $b \neq 0 \in R$, for $b = 0 \Rightarrow b_n^{m+1} = 0 \Rightarrow b_n = 0$ (by (1)) ∴ which is a Contradiction.

we have $a_0b = 0$

Now $a_1b = a_1b_n^{m+1} = (a_1b_n^m)\cdot b_n = 0 \cdot b_n = 0$,

$a_{m-1}b = a_{m-1}b^{m+1} = (a_{m-1}b_n^2)(b_n^{m-1}) = 0 \cdot b_n^{m-1} = 0$

$a_mb = a_mb_n^{m+1} = (a_mb_n^2)(b_n^m) = 0 \cdot b_n^m = 0$.

∴ $a_0b = a_1b = \cdots = a_mb = 0$

Hence $ba_0 = ba_1 = \cdots = ba_m = 0$, since R is commutative.

Note: The above Problem Can also be done by dropping the assumption that R has no non-zero nilpotent elements as proved below.

→ Let R be a Commutative ring. If $f(x)=a_0+a_1x+\cdots+a_mx^m$ in $R[x]$ is a zero divisor, Prove that there is an element $b\neq 0$ in R such that.

$$ba_0 = ba_1 = \cdots = ba_m = 0$$

Sol^n: Since $f(x)\in R[x]$ is a zero divisor, there exists some $g(x)\in R[x]$ of least positive degree such that

$$f(x)\,g(x)=0 \qquad \text{——— (1)}$$

It means that for all polynomials $h(x)\in R[x]$ with $\deg h(x) < \deg g(x)$ and satisfying $f(x)h(x)=0$, then $h(x)=0$. ——— (2)

Let $g(x) = b_0+b_1x+\cdots+b_nx^n \in R[x]$

we may suppose that $a_m\neq 0$ and $b_n\neq 0\in R$. we have

$$(a_0+a_1x+\cdots+a_{m-1}x^{m-1}+a_mx^m)(b_0+b_1x+\cdots+b_{n-1}x^{n-1}+b_nx^n)$$
$$= 0+0x+0x^2+\cdots \quad (2)$$

Let $h(x) = a_m g(x) = a_mb_0 + a_mb_1x + \cdots + a_mb_{n-1}x^{n-1}$

$\Rightarrow \deg h(x) \le n-1 < \deg g(x)$ and $f(x)h(x)=f(x)(a_mg(x))$ $(\because a_mb_n=0)$

$f(x)h(x) = a_m(f(x)g(x))$, Since R is Commutative.

$\therefore f(x)h(x)=0$, (by(1)) and $\deg h(x) < \deg g(x)=n$

In view of (2), it follows that, $h(x)=0$ i.e. $a_m g(x)=0$

from (2), $a_{m-1}b_n + a_mb_{n-1} = 0$

$\Rightarrow (a_{m-1}b_n + a_mb_{n-1})\,g(x) = 0\cdot g(x)$

$\Rightarrow b_n(a_{m-1}g(x)) + b_{n-1}(a_mg(x)) = 0$, Since R is Commutative

$\Rightarrow b_n(a_{m-1}g(x)) = 0$, as $a_m g(x) = 0$

$\Rightarrow a_{m-1}g(x) = 0$. Since $b_n \neq 0$. Again, from (1), we obtain

$a_{m-2}g(x) + a_{m-1}b_{n-1} + a_m b_{n-2} = 0 \Rightarrow a_{m-2}g(x) = 0$

Since $a_m g(x) = 0$ and $a_{m-1}g(x) = 0$

Proceeding in the similar manner, we obtain

$a_m g(x) = 0$, $a_{m-1}g(x) = 0 \cdots$, $a_1 g(x) = 0$, $a_0 g(x) = 0$.

In particular.

$a_m b_n = 0$, $a_{m-1}b_n = 0, \cdots a_1 b_n = 0$, $a_0 b_n = 0$; where $b_n \neq 0$.

Taking $b = b_n \neq 0 \in R$, and since R is commutative, we get

$ba_0 = ba_1 = \cdots = ba_m = 0$

⇒ In order for $F[x]$ to be a Euclidean ring with the degree function acting as the d-function of euclidean ring we still need that given $f(x), g(x) \in F[x]$, there exist $t(x), r(x)$ in $F[x]$ such that $f(x) = t(x)g(x) + r(x)$ where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$. This is provided us by

IAS-2017 2019

LEMMA (THE DIVISION ALGORITHM) :-
Let $f(x)$ and $g(x)$ be two non-zero polynomials in $F[x]$ (F being a field), then $\exists$ unique polynomials $t(x)$ and $r(x)$ in $F[x]$ such that $f(x) = t(x)g(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

Sol Let us consider the set

$$S = \{ f(x) - h(x)g(x) \mid h(x) \in F[x] \}.$$

for $0(x) \in F[x]$,
$f(x) = f(x) - 0(x).g(x) \in S$.
$\therefore S \neq \phi$.

Let $0 \in S$. Then by definition of S,
$\exists\ q(x) \in F[x]$ so that $0 = f(x) - q(x)g(x)$
i.e. $f(x) = q(x)g(x) + 0(x)$
i.e $f(x) = q(x)g(x) + r(x)$ where $r(x) = 0$.
$\therefore$ the theorem is proved.

Let $0(x) \notin S$. Then every polynomial in S is a non-zero polynomials and hence non-negative degree.
Let $r(x) \in S$ be a polynomial of least degree.
By definition of S, there exist $q(x) \in F[x]$ so that

$$r(x) = f(x) - q(x)g(x)$$
$$\text{i.e } f(x) = q(x)q(x) + r(x) \quad \text{---(1)}$$

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

So that $\deg g(x) = n$

NOW we have to prove that $\deg r(x) < n$.

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

If possible, suppose that $m = \deg r(x) \geq n$.

Let $r(x) = c_0 + c_1x + c_2x^2 + \cdots + c_mx^m$, $c_m \neq 0$.

NOW we have

$$c_m a_n^{-1} x^{m-n} g(x) = c_m a_n^{-1} x^{m-n} \left[a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + a_nx^n\right].$$

$$= c_m a_n^{-1} a_0 x^{m-n} + c_m a_n^{-1} a_1 x^{m-n+1} + \cdots + c_m a_n^{-1} a_{n-1} x^{m-1} + c_m x^m.$$

$\therefore r(x) = c_m a_n^{-1} x^{m-n} g(x)$

$$= (c_{m-1}x^{m-1} + \cdots + c_0) - \left(c_m a_n^{-1} a_{n-1} x^{m-1} + \cdots + c_m a_n^{-1} a_0 x^{m-n}\right)$$

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

where $\alpha(x) = (c_{m-1} - c_m a_n^{-1} a_{n-1}) x^{m-1} + \cdots + c_0$

$\Rightarrow \deg \alpha(x) \leq m-1$.

i.e $\deg \alpha(x) \leq \deg r(x) - 1$

i.e $\deg \alpha(x) < \deg r(x)$.

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

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

$$= f(x) - g(x)\beta(x),$$

where $\beta(x) = q(x) + c_m a_n^{-1} x^{m-n} \in F[x]$.

$\therefore \alpha(x) \in S$.

NOW we have $\alpha(x), r(x) \in S$ and $\deg \alpha(x) < \deg r(x)$.

This is a contradiction since $r(x)$ is the polynomial of least degree in S.

$\therefore$ Our supposition is wrong.

Hence $\deg r(x) < n$

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

$\therefore \exists\ q(x), r(x) \in F[x]$ s.t that

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

Uniqueness of $q(x)$ and $r(x)$:-

If possible, suppose that $f(x) = q'(x)g(x) + r'(x)$ where $r'(x) = 0$ or $\deg r'(x) < \deg g(x)$.

Then $q(x)g(x) + r(x) = q'(x)g(x) + r'(x)$

i.e $(q(x) - q'(x))g(x) = r'(x) - r(x)$

If $q(x) - q'(x) \neq 0$ then $\deg(q(x) - q'(x))g(x) = \deg(q(x) - q'(x)) + \deg g(x)$

i.e $\deg(r'(x) - r(x)) \geq \deg g(x)$.

This is a contradiction because $\deg r(x) < \deg g(x)$ and $\deg r'(x) < \deg g(x)$

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

$\Rightarrow q'(x) = q(x)$ & $r'(x) = r(x)$.

Hence $q(x), r(x) \in F[x]$ are unique.

Note: (1). The polynomials $q(x)$ and $r(x)$ of the above theorem are called the quotient and the remainder.

(2). In the above theorem if $r(x)=0$ then we say that $g(x)$ divides $f(x)$ or $g(x)$ is a factor of $f(x)$.

→ If F is a field, then $F[x]$ is a Euclidean domain.

Sol: Let F be a field

Then F is an ID

$\therefore F[x]$ is an ID.

further for any two non-zero polynomials $f(x)$ and $g(x)$ in $R[x]$,

we have $\deg(f(x)\cdot g(x)) = \deg f(x) + \deg g(x)$

$\geq \deg f(x)$.

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

$\therefore \deg f(x) \leq \deg(f(x)g(x))$ ——— (1)

NOW we define the Euclidean valuation d on $F[x]$ as follows: $d(f) = d(f(x))$ $\forall$ $f(x) \neq 0 \in F[x]$. ——— (2)

Then $d(f)$ is a non-negative integer, ——— (3)

since $\deg f(x)$ is so.

from (1) and (2), we see that

$\deg(f) \leq \deg(fg)$ $\forall$ $f \neq 0, g \neq 0$ in $F[x]$

$\therefore$ By Division algorithm,

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

such that $f(x) = t(x)g(x) + r(x)$, where

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

$\therefore f = tg + r$, where $r = 0$ or $d(f) < d(g)$.

Hence $F[x]$ is a Euclidean domain.

→ If F is a field, $F[x]$ is a principal ideal domain.

Sol^n: Let U be an ideal of $F[x]$ and $U = \{0\}$ where 0 is the zero polynomials.

Then $U = \langle 0 \rangle$, the principal ideal generated by '0'.

Let U be an ideal of $F[x]$ and $U \neq \{0\}$.

Then U contains polynomials of non-negative degree.

By well ordering principle $\exists$ a polynomial $f(x) \in U$, $f(x) \neq 0$ such that $\deg f(x) \leq \deg g(x)$ where $g(x)$ is any polynomial in U and $g(x) \neq f(x)$.

Let $h(x)$ be any polynomial in U.

By the division algorithm, $\exists$ polynomials $q(x), r(x)$ in $F[x]$ such that

$h(x) = f(x)q(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg f(x)$.

$f(x) \in U$, $q(x) \in F[x]$, U is an ideal $\Rightarrow f(x)q(x) \in U$

$h(x) \in U$, $f(x)q(x) \in U \Rightarrow h(x) - f(x)q(x) = r(x) \in U$

Now $r(x) \in U$, $r(x) = 0$ or $\deg r(x) < \deg f(x)$

$\Rightarrow r(x) = 0$

$\therefore h(x) = f(x)q(x)$ where $q(x) \in F[x]$.

$\therefore U = \{ f(x)q(x) / q(x) \in F[x] \} = \langle f(x) \rangle$ is the principal ideal generated by $f(x)$.

Hence every ideal U of $F[x]$ is a principal ideal.

→ $\mathbb{Z}[x]$ over the ring of integers is not a principal ideal ring.

Remarks: It may be observed that any ideal A of $F[x]$ is expressible as $A = \langle p(x) \rangle = \{ p(x) f(x) / f(x) \in F[x] \}$. In particular, $\langle x \rangle = \{ x f(x) / f(x) \in F[x] \}$, for some $p(x) \in A$ i.e., $A = \langle p(x) \rangle$.

Soln: Let $S=\{x,2\}\subset Z[x]$ be a subset containing two elements.

we show that ideal generated by $S=(x,2)$ is not a principal ideal of $Z[x]$.

If possible, let $(x,2)$ be a principal ideal of $Z[x]$.

$\therefore \exists\ a(x)\in Z[x]$ so that $(x,2)=[a(x)]$

$x\in[a(x)] \Rightarrow \exists\ b(x)\in Z[x]$ so that $x=a(x)\,b(x)$ ——— (1)

$2\in[a(x)] \Rightarrow \exists\ c(x)\in Z[x]$ so that $2=a(x)\,b(x)$ ——— (2)

$\therefore \deg[a(x)\,b(x)]=\deg x \Rightarrow \deg a(x)+\deg b(x)=1$ ——— (3)

$\deg[a(x)\,c(x)]=\deg 2 \Rightarrow \deg a(x)+\deg c(x)=0$ ——— (4)

From (4); $\deg a(x)=0$ and $\deg c(x)=0$

$\Rightarrow a(x), c(x)$ are non-zero constant polynomials.

$\Rightarrow a(x), c(x)$ are non-zero integers.

Again, $a(x)\cdot c(x)=2 \Rightarrow a(x), c(x)$ are non-zero integers with the following four alternatives.

$a(x)=1,\ c(x)=2$

$a(x)=-1,\ c(x)=-2$

$a(x)=2,\ c(x)=1$

$a(x)=-2,\ c(x)=-1$

If $a(x)=\pm 1$, we have, $[a(x)]=Z[x]$

This is a contradiction to $[a(x)]=(x,2)$.

Again, if $a(x)=\pm 2$ then from (2)

$x=a(x)\,c(x) \Rightarrow x=\pm 2(c_0+c_1x+\cdots)$.

$\Rightarrow 1=\pm 2c_1$ where $c_1\in Z$

This is also a contradiction as there exists no integers c_1.

so that $1=\pm 2c_1$.

$\therefore$ Our supposition that $(x,2)$ is a principal ideal is wrong.

Hence $Z[x]$ is not a principal ideal ring.

→ The ideal $A = \langle p(x) \rangle$ in $F[x]$ is a maximal ideal iff $p(x)$ is an irreducible element of $F[x]$.

Soln: The result follows by known theorem (If F is a field, $F[x]$ is a principal ideal domain.) and (Let R be a PID, which is not a field. Then an ideal $A = \langle a \rangle$ is a maximal ideal iff a is an irreducible element of R)

→ $\frac{F\langle x \rangle}{\langle f(x) \rangle}$ is a field iff $p(x)$ is an irreducible element of $F[x]$.

Soln: Since $F[x]$ is a commutative ring with unity the result follows by the theorem (The ideal $A = \langle p(x) \rangle$ in $F[x]$ is a maximal ideal iff $p(x)$ is an ireducible element of $F[x]$.) and the theorem (If R is commutative ring with unity, then an ideal M of R is maximal iff R/M is a field.)

→ Show that $\langle x+2 \rangle$ is a maximal ideal of $\mathbb{Q}[x]$ and hence $\frac{\mathbb{Q}[x]}{\langle x+2 \rangle}$ is a field.

Soln: By known theorem [If f is a field, $F[x]$ is a principal ideal domain.]

$\therefore \mathbb{Q}[x]$ is a P.I.D.

we have $\langle x+2 \rangle = \{ (x+2) f(x) / f(x) \in \mathbb{Q}[x] \}$

$\langle x+2 \rangle$ is a maximal ideal of $\mathbb{Q}[x]$, if we prove that $x+2$ is an irreducible element of $\mathbb{Q}[x]$.

Let $x+2 = f(x)\, g(x)$

where $f(x), g(x) \in \mathbb{Q}[x]$ ——— (1)

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

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

This gives us two cases.

Case(1): $\deg f(x) = 0$ and $\deg g(x) = 1$

Case(2): $\deg f(x) = 1$ and $\deg g(x) = 0$

In case (1), we may take

$f(x) = a_0 \neq 0 \in \mathbb{Q}$ and $g(x) = b_0 + b_1 x$; $b_0 \in \mathbb{Q}$, $b_1 \neq 0 \in \mathbb{Q}$.

putting in (1), we get

$$x + 2 = a_0(b_0 + b_1 x)$$

$\Rightarrow a_0 b_0 = 2$ and $a_0 b_1 = 1$, $a_0 \neq 0$, $b_1 \neq 0 \in \mathbb{Q}$.

Now $a_0 b_1 = 1 \Rightarrow a_0 / 1 \Rightarrow f(x) = a_0$ is a unit.

Thus $x+2$ is an irreducible element of $\mathbb{Q}[x]$.

Similarly, in case (2) we can prove that $g(x)$ is a unit and $x+2$ is an irreducible element of $\mathbb{Q}[x]$.

Hence $\langle x+2 \rangle$ is a maximal ideal of $\mathbb{Q}[x]$.

Since $\mathbb{Q}[x]$ is a commutative ring with unity, $\frac{\mathbb{Q}[x]}{\langle x+2 \rangle}$ is a field.

→ Show that $\langle x+1 \rangle$ is a maximal ideal of $\mathbb{Q}[x]$ and that $\frac{\mathbb{Q}[x]}{\langle x+1 \rangle}$ is a field.

Example 3.2.11. *If R is a ring, prove that $\frac{R[x]}{\langle x \rangle} \approx R$, $\langle x \rangle$ is the ideal generated by x.* [D.U., 1997]

Solution. We have

$$\langle x \rangle = \{x\, p(x) : p(x) \in R[x]\}.$$

We define a mapping

$$\theta : R[x] \to R \text{ as } \theta(f(x)) = \theta(a_0 + a_1 x + \ldots + a_n x^n) = a_0. \quad \ldots(1)$$

Obviously, θ is onto. Now we show that θ is a homomorphism.

Let $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in R[x]$,

and $g(x) = b_0 + b_1 x + \ldots + b_m x^m \in R[x]$.

Then $f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \ldots$,

and $f(x)\, g(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \ldots$

From (1), we have

$$\theta(f(x) + g(x)) = a_0 + b_0 = \theta(f(x)) + \theta(g(x)),$$

$$\theta(f(x)\, g(x)) = a_0 b_0 = \theta(f(x))\, \theta(g(x)).$$

Thus θ is a homomorphism of $R[x]$ onto R.

By Fundamental theorem of homomorphism, we can write

$$\frac{R[x]}{Ker\,\theta} \approx R. \quad \ldots(2)$$

Let $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ be an arbitrary element of $Ker\,\theta$.

Then $f(x) \in Ker\,\theta \Leftrightarrow \theta(f(x)) = 0 \Leftrightarrow a_0 = 0$

$\Leftrightarrow f(x) = a_1 x + a_2 x^2 + \ldots + a_n x^n$

$\Leftrightarrow f(x) = x(a_1 + a_2 x + \ldots + a_n x^{n-1})$.

$\Leftrightarrow f(x) \in \langle x \rangle \Leftrightarrow Ker\,\theta = \langle x \rangle$.

Putting in (2), we get $\frac{R[x]}{\langle x \rangle} \approx R$.

Example 3.2.12. *If R is a commutative ring with unity and A is an ideal of R, prove that*

$$\frac{R[x]}{A[x]} \approx \frac{R}{A}[x].$$

Deduce that if A is a prime ideal of R, then $A[x]$ is a prime ideal of $R[x]$. [D.U., 1992]

Solution. Since A is an ideal of R, the quotient ring R/A is a commutative ring with unity, where

$$\frac{R}{A} = \{\bar{r} = r + A : r \in R\}.$$

It follows that $\frac{R}{A}[x]$ is also a commutative ring with unity.

We define a mapping

$$\theta : R[x] \to \frac{R}{A}[x] \text{ as}$$

$$\theta(f(x)) = \theta(r_0 + r_1 x + \ldots + r_n x^n) = \bar{r}_0 + \bar{r}_1 x + \ldots + \bar{r}_n x^n. \qquad \ldots(1)$$

(Here $\bar{r}_i = r_i + A,\ r_i \in R$)

We shall prove that θ is a homomorphism.

Let $f(x) = r_0 + r_1 x + \ldots + r_n x^n \in R[x]$,

and $g(x) = s_0 + s_1 x + s_m x^m \in R[x]$.

Then $f(x) + g(x) = r_0 + s_0 + (r_1 + s_1) x + \ldots,$

$f(x)\, g(x) = r_0 s_0 + (r_0 s_1 + r_1 s_0) x + \ldots$

From (1), we have

$$\theta(f(x) + g(x)) = \overline{r_0 + s_0} + (\overline{r_1 + s_1})\, x + \ldots \qquad \ldots(2)$$

$$\theta(f(x)\, g(x)) = \overline{r_0 s_0} + (\overline{r_0 s_1 + r_1 s_0})\, x + \ldots \qquad \ldots(3)$$

We see that

$$\overline{r_i + s_i} = r_i + s_i + A = (r_i + A) + (s_i + A) = \bar{r}_i + \bar{s}_i, \text{ for each } i.$$

Again $\overline{r_i s_j} = r_i s_j + A = (r_i + A)(s_j + A) = \bar{r}_i \bar{s}_j$, for each i and j

Using these results in (2) and (3), we get

$$\theta(f(x) + g(x)) = \bar{r}_0 + \bar{s}_0 + (\bar{r}_1 + \bar{s}_1)\, x + \ldots$$

$$= (\bar{r}_0 + \bar{r}_1 x + \ldots) + (\bar{s}_0 + \bar{s}_1 x + \ldots)$$

$$= \theta(f(x)) + \theta(g(x)), \text{ by (1)}$$

$$\theta(f(x)\, g(x)) = (\bar{r}_0 \bar{s}_0) + (\bar{r}_0 \bar{s}_1 + \bar{r}_1 \bar{s}_0)\, x + \ldots$$

$$= (\bar{r}_0 + \bar{r}_1 x + \ldots.)\,(\bar{s}_0 + \bar{s}_1 x + \ldots)$$

$$= \theta(f(x))\, \theta(g(x)), \text{ by (1)}.$$

Thus θ is a homomorphism. Also θ is onto, for any $p(x) \in \frac{R}{A}[x] \Rightarrow p(x) = \bar{t}_0 + \bar{t}_1 x + \ldots + \bar{t}_k x^k$, where $\bar{t}_i = t_i + A\ (t_i \in R) \Rightarrow \theta(q(x)) = p(x)$, where $q(x) = t_0 + t_1 x + \ldots + t_k x^k \in R[x]$.

By Fundamental theorem of homomorphism, we obtain

$$\frac{R[x]}{Ker\, \theta} \approx \frac{R}{A}[x]. \qquad \ldots(4)$$

Let $f(x) = r_0 + r_1 x + ... + r_n x^n \in Ker\,\theta$ be arbitrary.

$\Leftrightarrow \theta(f(x)) = \bar{0} \in \frac{R}{A}[x]$ $(\bar{0} = A)$

$\Leftrightarrow \bar{r}_0 + \bar{r}_1 x + ... + \bar{r}_n x^n = \bar{0} + \bar{0}\,x + ... + \bar{0}\,x^n$, by (1)

$\Leftrightarrow \bar{r}_i = \bar{0}$, for each i

$\Leftrightarrow r_i + A = A$, for each i

$\Leftrightarrow r_i \in A$, for each i

$\Leftrightarrow f(x) = r_0 + r_1 x + ... + r_n x^n \in A[x]$

$\Leftrightarrow Ker\,\theta = A[x]$.

Putting in (4), we get

$$\frac{R[x]}{A[x]} \approx \frac{R}{A}[x]. \qquad ...(5)$$

(*ii*) Let A be a prime ideal of R.

Then $\frac{R}{A}$ is an integral domain. [Theorem 2.6.3]

$\Rightarrow \frac{R}{A}[x]$ is an integral domain. [Cor. 3 of Theorem 3.2.1]

$\Rightarrow \frac{R[x]}{A[x]}$ is an integral domain, by (5)

$\Rightarrow A[x]$ is a prime ideal of $R[x]$. [Theorem 2.6.3]

Example 3.2.13. *Prove that the ideal* $\langle x^4 + 4 \rangle$ *is not a prime ideal of* $\mathbf{Q}[x]$, $\mathbf{Q}$ *being the field of rational numbers.*

Solution. We have $\langle x^4 + 4 \rangle = \{(x^4 + 4) f(x) : f(x) \in \mathbf{Q}[x]\}$

and $(x^2 + 2 + 2x)(x^2 + 2 - 2x) = (x^2 + 2)^2 - 4x^2 = x^4 + 4$.

Thus $(x^2 + 2x + 2)(x^2 - 2x + 2) \in \langle x^4 + 4 \rangle$, but

$x^2 + 2x + 2 \notin \langle x^4 + 4 \rangle$ and $x^2 - 2x + 2 \notin \langle x^4 + 4 \rangle$.

Hence $\langle x^4 + 4 \rangle$ is not a prime ideal of $\mathbf{Q}[x]$.

Theorem 3.2.8. *An integral domain R with unity is a field if and only if $R[x]$ is a principal ideal domain.* [D.U., 1997]

Proof. *Condition is necessary*

Let R be a field. Then $R[x]$ is a Euclidean domain. [Theorem 3.2.5]

Hence $R[x]$ is a principal ideal domain [E.D. $\Rightarrow$ P.I.D.]

Condition is sufficient

Let $R[x]$ be a principal ideal domain.

We shall prove that R is a field. By Example 3.2.11, we have

$$\frac{R[x]}{\langle x \rangle} \approx R. \qquad ...(1)$$

We now proceed to show that

$$\langle x \rangle = \{x\,p(x) : p(x) \in R[x]\}$$

is a maximal ideal of $R[x]$. Let M be any ideal of $R[x]$ such that

$$\langle x \rangle \subseteq M \subseteq R[x]. \qquad \ldots(2)$$

Since $R[x]$ is a P.I.D., M is a principal ideal of $R[x]$.

Let $M = \langle f(x) \rangle$, for some $f(x) \in M$. $\ldots(3)$

We have $x = x \cdot 1$ and so $x \in \langle x \rangle$

$\Rightarrow x \in M$, by (2)

$\Rightarrow x = f(x)\,g(x)$, for some $g(x) \in R[x]$, by (3).

This gives rise to the following cases :

Case I. $f(x) = 1$ and $g(x) = x$.

Case II. $f(x) = x$ and $g(x) = 1$.

In case I, $M = \langle 1 \rangle = R[x]$.

In case II, $\langle f(x) \rangle = \langle x \rangle \Rightarrow M = \langle x \rangle$.

It follows that $\langle x \rangle$ is a maximal ideal of $R[x]$, where $R[x]$ is a commutative ring with unity. Hence $\dfrac{R[x]}{\langle x \rangle}$ is a field [Theorem 2.6.1.] and so by (1), R is a field.

Corollary 1. $\mathbf{Z}[x]$ *is not a P.I.D.*

Proof. Let, if possible, $\mathbf{Z}[x]$ be a P.I.D., where $\mathbf{Z}$ is an integral domain with unity. By Theorem 3.2.8, $\mathbf{Z}$ is a field which is impossible. Hence $\mathbf{Z}[x]$ is not a P.I.D.

Corollary 2. *If F is a field, then $F[x, y]$ is not a P.I.D.*

Proof. $F[x, y]$ is a polynomial ring (over F) in two indeterminates x and y. A typical element of $F[x, y]$ is of the form

$$a_0 + a_1x + a_2y + b_1x^2 + b_2xy + b_3y^2 + \ldots + \alpha_1 x^{n-1} + \alpha_2 x^{n-1} y + \ldots + \alpha_n y^n,$$

where $a_i, b_i, \ldots, \alpha_i \in F$ and n is a non-negative integer.

It is easy to verify that

$$F[x, y] = F_1[y], \text{ where } F_1 = F[x].$$

Let, if possible, $F[x, y]$ be a P.I.D. $\Rightarrow F_1[y]$ is a P.I.D., where $F_1 = F[x]$ is an integral domain with unity

$\Rightarrow F_1$ is a field. [See Theorem 3.2.8.]

$\Rightarrow F[x]$ is a field, which is not true as x is not invertible.

Hence $F[x, y]$ is not a P.I.D.

Remark. *For an independent proof of Corollary 2, see Example* 3.2.21.

EXAMPLES

Example 3.2.14. *R is a ring such that $R[x]$ is a P.I.D. Show that R is a field.* [... U., 1991]

Solution. Since $R[x]$ is a P.I.D., $R[x]$ is an integral domain with unity (by definition). Consequently, R is an integral domain with unity [See Example 3.2.5]. The result follows by the sufficient condition of Theorem 3.2.8.

Example 3.2.15. *Prove that if R is an integral domain with unity that is not a field, then $R[x]$ is not a P.I.D.*

Solution. Let, if possible, $R[x]$ be a P.I.D. By Theorem 3.2.8, R is a field, which is a contradiction. Hence $R[x]$ is not a P.I.D.

Example 3.2.16. *Prove that if D is an integral domain with unity that is not a field, then $D[x]$ is not a Euclidean domain.*

Solution. Let, if possible, $D[x]$ be a Euclidean domain. Then $D[x]$ is a P.I.D. and so by Theorem 3.2.8, D is a field, which is a contradiction. Hence $D[x]$ is not a Euclidean domain.

Example 3.2.17. *Show that*

$$A = \{x f(x) + 2g(x) : f(x), g(x) \in \mathbf{Z}[x]\}$$

is not a principal ideal of $\mathbf{Z}[x]$ and so $\mathbf{Z}[x]$ is not a P.I.D.

Solution. Firstly, we show that A is an ideal of $\mathbf{Z}[x]$. Let $h(x), k(x) \in A$. Then

$$h(x) = x f_1(x) + 2 g_1(x),\ k(x) = x f_2(x) + 2 g_2(x),$$

for some $f_1(x), f_2(x), g_1(x), g_2(x)$ in $\mathbf{Z}[x]$. We have

$$h(x) - k(x) = x(f_1(x) - f_2(x)) + 2(g_1(x) - g_2(x)) \in A.$$

For any $h(x) \in A$ and $r(x) \in \mathbf{Z}[x]$, we have

$$h(x)\, r(x) = x f_1(x)\, r(x) + 2 g_1(x)\, r(x) \in \mathbf{Z}[x].$$

Thus A is an ideal of $\mathbf{Z}[x]$. Now we show that A is not a principal ideal of $\mathbf{Z}[x]$. Let, if possible, $A = \langle p(x) \rangle$, for some $p(x) \in A$. We can write

$$x = x(1 + 0x + 0x^2 + \ldots) + 2(0 + 0x + 0x^2 + \ldots) \text{ and so } x \in A.$$

$$\therefore \quad x \in \langle p(x) \rangle \Rightarrow x = p(x)\, s(x), \text{ for some } s(x) \in \mathbf{Z}[x].$$

Similarly, $2 \in A = \langle p(x) \rangle \Rightarrow 2 = p(x)\, t(x)$, for some $t(x) \in \mathbf{Z}[x]$. ...(1)

From the above relations, we get

$$2x = 2p(x)\, s(x) \text{ and } 2x = xp(x)\, t(x)$$

$$\Rightarrow \quad 2p(x)\, s(x) = x\, p(x)\, t(x)$$

$$\Rightarrow \quad x\, t(x) = 2s(x)$$

$\Rightarrow$ each coefficient of $x\, t(x)$ and hence that of $t(x)$ is an even integer.

Let $t(x) = 2r(x)$, for some $r(x) \in \mathbf{Z}[x]$. ...(2)

From (1) and (2), we obtain

$$p(x)\, r(x) = 1 \Rightarrow 1 \in A = \langle p(x) \rangle$$

$$\Rightarrow 1 \in \{x f(x) + 2g(x) : f(x), g(x) \in \mathbf{Z}[x]\}$$

$$\Rightarrow 1 = x(a_0 + a_1 x + \ldots) + 2(b_0 + b_1 x + \ldots) \text{ ; for some } a_i, b_i \in \mathbf{Z}$$

$\Rightarrow 1 = 2b_0$ ($b_0 \in \mathbf{Z}$), which is impossible.

Hence A is not a principal ideal of $\mathbf{Z}[x]$. Consequently, $\mathbf{Z}[x]$ is not a P.I.D.

Example 3.2.18. *Prove that the ideal* $\langle x \rangle$ *of* $\mathbf{Z}[x]$ *is a prime ideal but not a maximal ideal of* $\mathbf{Z}[x]$.

Solution. We have $\langle x \rangle = \{x\,p(x) : p(x) \in \mathbf{Z}[x]\}$.

Let $f(x) = a_0 + a_1x + \ldots + a_m x^m$ and $g(x) = b_0 + b_1x + \ldots + b_nx^n$ be two polynomials in $\mathbf{Z}[x]$ such that $f(x)\,g(x) \in \langle x \rangle$. Then

$f(x)\,g(x) = x\,p(x)$, for some $p(x) = c_0 + c_1x + \ldots + c_r x^r \in \mathbf{Z}[x]$.

We have

$$(a_0 + a_1x + \ldots)(b_0 + b_1x + \ldots) = x(c_0 + c_1x + \ldots).$$

Comparing the constant term on both the sides, we get

$$a_0b_0 = 0 \implies a_0 = 0 \text{ or } b_0 = 0. \qquad (\because a_0, b_0 \in \mathbf{Z})$$

If $a_0 = 0$, then $f(x) = a_1x + a_2x^2 + \ldots + a_m x^m$

$$= x(a_1 + a_2x + \ldots + a_m x^{m-1}) \in \langle x \rangle.$$

Similarly, $b_0 = 0 \Rightarrow g(x) \in \langle x \rangle$.

Hence $\langle x \rangle$ is a prime ideal of $Z[x]$.

However, $\langle x \rangle$ is not a maximal ideal of $\mathbf{Z}[x]$, since

$$A = \{x f(x) + 2g(x) : f(x), g(x) \in \mathbf{Z}[x]\}$$

is a proper ideal of $\mathbf{Z}[x]$ such that

$$\langle x \rangle \subset A \subset \mathbf{Z}[x].$$

Notice that $2 \in A$ but $2 \notin \langle x \rangle$ and $1 \in \mathbf{Z}[x]$ but $1 \notin A$.

[By Example 3.2.17, $1 \in A \Rightarrow 1 = 2b_0$ $(b_0 \in \mathbf{Z})$, a contradiction].

Example 3.2.19. *Show that greatest common divisor of* 2 *and* x *in* $\mathbf{Z}[x]$ ($\mathbf{Z}$ = *ring of integers*) *cannot be written as* $2r(x) + xs(x)$, *where* $r(x), s(x) \in \mathbf{Z}[x]$. *Hence show that* $\mathbf{Z}[x]$ *is not a P.I.D..* [D.U., 1991]

Solution. Let $f(x)$ be a g.c.d. of 2 and x in $\mathbf{Z}[x]$ [g.c.d. of any two non-zero elements exists in $\mathbf{Z}[x]$, since $\mathbf{Z}[x]$ is a unique factorization domain. [See Theorem 3.3.4.]

Let, if possible, $f(x) = 2r(x) + xs(x)$, ...(1)

where $r(x), s(x) \in \mathbf{Z}[x]$ and $f(x) = (2, x)$.

By definition of g.c.d., $f(x) \mid 2$ and $f(x) \mid x$

$\Rightarrow$ $2 = f(x)\,g(x)$ and $x = f(x)\,h(x)$, for some $g(x), h(x) \in \mathbf{Z}[x]$.

We have $deg\,(f(x)\,g(x)) = deg\,2 = 0$

$\Rightarrow deg\,f(x) + deg\,g(x) = 0$, since $\mathbf{Z}$ is an I.D.

$\Rightarrow deg\,f(x) = 0 \Rightarrow f(x)$ is a constant polynomial.

Let $f(x) = \alpha$, where $\alpha \neq 0 \in \mathbf{Z}$.

$\therefore$ $x = \alpha\,h(x) \implies deg\,h(x) = 1$.

Let $h(x) = \beta x + \gamma$, where $\beta \neq 0 \in \mathbf{Z}$, $\gamma \in \mathbf{Z}$.

We have $x = \alpha(\beta x + \gamma) = \alpha\beta x + \alpha\gamma \Rightarrow \alpha\beta = 1 \Rightarrow 1 = f(x)\,\beta$.

Using (1), $1 = [2r(x) + xs(x)]\,\beta$.

Comparing the constant term on both the sides, we get

$$1 = 2a_0 \beta, \qquad \ldots(2)$$

where $r(x) = a_0 + a_1 x + \ldots \in \mathbf{Z}[x]$, $a_0 \neq 0 \in \mathbf{Z}$.

Notice that if $a_0 = 0$, then by (2), $1 = 0$, a contradiction.

The equation (2) is impossible in $\mathbf{Z}$, since a_0 and $\beta \in \mathbf{Z}$. Hence $f(x)$ cannot be written as $2r(x) + xs(x)$, where $f(x) = (2, x)$.

(*ii*) Let, if possible, $\mathbf{Z}[x]$ be a P.I.D.

Then the ideal $A = \{2r(x) + xs(x) : r(x), s(x) \in \mathbf{Z}[x]\}$ of $\mathbf{Z}[x]$ is principal and so $A = \langle p(x) \rangle$, for some $p(x) \in A$.

It follows that $p(x) = 2r(x) + xs(x)$, for some $r(x), s(x) \in \mathbf{Z}[x]$.

The above relation implies that $p(x)$ is g.c d of 2 and x. But this is impossible, as proved above.

Hence A is not a principal ideal of $\mathbf{Z}[x]$ and so $\mathbf{Z}[x]$ is not a P.I.D.

Example 3.2.20. *Show that the ideal*

$$A = \{xf(x) + 2g(x) : f(x), g(x) \in \mathbf{Z}[x]\}$$

is a maximal ideal of $\mathbf{Z}[x]$

Solution. Let M be any ideal of $\mathbf{Z}[x]$ such that

$$A \subset M \subset \mathbf{Z}[x], A \neq M.$$

Then there exists some $p(x) \in M$ such that $p(x) \notin A$.

Let $p(x) = a_0 + a_1 x + \ldots + a_m x^m \in \mathbf{Z}[x]$

If a_0 is even, then $a_0 = 2k$, for some $k \in \mathbf{Z}$.

$\therefore$ $p(x) = x(a_1 + a_2 x + \ldots + a_m x^{m-1}) + 2k \in A$,

which is a contradiction. Thus a_0 is an odd integer, say $a_0 = 2a + 1$, $a \in \mathbf{Z}$.

$\therefore$ $p(x) = 2a + 1 + a_1 x + \ldots + a_m x^m = q(x) + 1$,

where $q(x) = 2a + a_1 x + \ldots + a_m x^m$

$= x(a_1 + a_2 x + \ldots + a_m x^{m-1}) + 2a \in A \subset M$.

Now $p(x) \in M$ and $q(x) \in M \Rightarrow p(x) - q(x) \in M$, since M is an ideal of $\mathbf{Z}[x] \Rightarrow 1 \in M \Rightarrow M = \mathbf{Z}[x]$.

Hence A is a maximal ideal of $\mathbf{Z}[x]$.

Example 3.2.21. *Show that* $F[x, y]$ *is not a P.I.D., F being a field.*

Solution. It is clear that $(x) = \{xf(x, y) : f(x, y) \in F[x, y]\}$ is an ideal of $F[x, y]$. Similarly, (y) is an ideal of $F[x, y]$. Consequently, $(x) + (y)$ is also an ideal of $F[x, y]$. Let, if possible,

$$(x) + (y) = \langle f(x, y) \rangle, \text{ for some } f(x, y) \in F[x, y].$$

Clearly, $x = x + 0 \in (x) + (y)$. Thus $x = af(x, y)$, for some $a \neq 0 \in F$.

Similarly, $y = bf(x, y)$, for some $b \neq 0 \in F$.

The above relations imply $xa^{-1} = yb^{-1} \Rightarrow bx - ay = 0$, which is absurd, as x and y are independent variables over F. Hence $F[x, y]$ is not a P.I.D.