STUDY MATERIALS

(RING THEORY-II)

TOPIC: PRINCIPAL IDEAL DOMAIN

Mathematics Honours
Semester – 6

Paper – C14T Unit - 1

Dr. Sangita Chakraborty
Associate Professor
Department of Mathematics
Kharagpur College

IDEALS of an I.D.

Theorem:- Let D be an I.D. and $a, b \in D$. Then

(i) $b|a$ if and only if $\langle a\rangle \subset \langle b\rangle$.

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

(iii) a is a unit in D iff $\langle a\rangle = D$.

Proof:-

(i) Suppose that $b|a$. Then $a = b.x$; for some $x \in D$.

$\therefore \forall r \in D,\ a.r = (b.x).r = b.(x.r)$, where $(x.r) \in D$.

$\Rightarrow \langle a\rangle \subset \langle b\rangle$.

Conversely, let $\langle a\rangle \subset \langle b\rangle$. Then $a \in \langle a\rangle \subset \langle b\rangle$.

$\therefore a \in \langle b\rangle \Rightarrow a = b.q$; for some $q \in D$.

$\Rightarrow b|a$.

(ii) Let a and b are associates. Then

$a|b$ and $b|a \Rightarrow \langle b\rangle \subset \langle a\rangle$ and $\langle a\rangle \subset \langle b\rangle$. [by (i)].

$\Rightarrow \langle a\rangle = \langle b\rangle$.

Conversely, let $\langle a\rangle = \langle b\rangle$. Then $\langle a\rangle \subset \langle b\rangle$, $\langle b\rangle \subset \langle a\rangle$.

$\langle a\rangle \subset \langle b\rangle \Rightarrow b|a$ and $\langle b\rangle \subset \langle a\rangle \Rightarrow a|b$. [by (i)].

$\therefore a|b$ and $b|a \Rightarrow$ a and b are associates

(iii) Let a be a unit in D. Then $\exists\ b \in D$ s.t. $a.b = I$,

where I is the unity in D.

Now $I = a.b$ where a is a unit $\Leftrightarrow$ a is associate of I.

$\Leftrightarrow \langle a\rangle = \langle I\rangle = D$. [by (ii)].

PRINCIPAL IDEAL DOMAIN (PID).

Let R be a commutative ring with unity.

A principal ideal generated by $a \in R$ is an ideal $\langle a\rangle = \{r.a : r \in R\}$.

Definition of PID:- An **I.D.** in which every ideal is a principal ideal is said to be a PID.

Examples:- ① The I.D. $\mathbb{Z}$ is a PID.

② A field F is an I.D., and is a PID.

Here the only ideals are:

$\{0\} = \langle 0\rangle$ and $F = \langle I\rangle$.

Th. Let D be a PID and $\langle p \rangle$ be a non-zero ideal in D. Then $\langle p \rangle$ is a maximal ideal iff p is irreducible.

Proof:- Suppose that $\langle p \rangle$ is a maximal ideal in D.
Let $a \in D$ and $a|p$. Then $\langle p \rangle \subset \langle a \rangle$; Also $\langle a \rangle \subset D$.
Since $\langle p \rangle$ is maximal, either $D = \langle a \rangle$ or $\langle p \rangle = \langle a \rangle$.
$\Rightarrow$ either a is a unit or a, p are associates.
$\therefore$ p is irreducible in D.
Conversely, let p be irreducible.
If $\langle a \rangle$ be an ideal in D s.t. $\langle p \rangle \subset \langle a \rangle \subset D$, then $a|p$.
Since p is irreducible, either a is a unit, or a, p are associates.
$\therefore$ either $\langle a \rangle = D$ or $\langle a \rangle = \langle p \rangle$
$\Rightarrow \langle p \rangle$ is a maximal ideal.

Cor:- In a PID D, an element p is a prime iff p is irreducible.

Proof:- Let p be a prime in a PID D.
$\therefore p \neq 0$ and p is not a unit in D.
Let $a \in D$ and $a|p$. Then $p = a \cdot b$ for some $b \in D$.
Now $p = a \cdot b \Rightarrow p | a \cdot b$, and since p is prime,
$\Rightarrow$ either $p|a$ or $p|b$.

(i) If $p|a$, then we have $a|p$ and $p|a$
$\Rightarrow a$ is an associate of p.

(ii) If $p|b$, then $b = p \cdot d$ for some $d \in D$.
$\therefore p = a \cdot b = a \cdot (p \cdot d) = p \cdot (a \cdot d)$
$\Rightarrow p \cdot (1 - a \cdot d) = 0 \Rightarrow 1 - a \cdot d = 0$ [$\because p \neq 0$ and D contains no divisor of zero]
$\Rightarrow a \cdot d = 1 \Rightarrow a$ is a unit in D.

$\therefore a|p \Rightarrow$ either a, p are associates or a is a unit
$\Rightarrow p$ is irreducible in D whenever p is prime there.

Conversely, Let p be irreducible in D and $p \mid a.b$ for some $a, b \in D$.

$\therefore \langle ab \rangle \subset \langle p \rangle \Rightarrow ab \in \langle p \rangle$.

Since p is irreducible, then if $\langle a \rangle$ is an ideal in D s.t. $\langle p \rangle \subset \langle a \rangle \subset D$, we have $a \mid p \Rightarrow$ either a is a unit or a, p are associates.

$\therefore$ either $\langle a \rangle = D$ or $\langle a \rangle = \langle p \rangle$.

$\Rightarrow \langle p \rangle$ is a maximal ideal.

Now every maximal ideal in D is also a prime ideal, since D is a commutative ring with unity.

$\therefore \langle p \rangle$ must be a prime ideal.

$\therefore ab \in \langle p \rangle \Rightarrow$ either $a \in \langle p \rangle$ or $b \in \langle p \rangle$

$\Rightarrow$ either $\langle a \rangle \subset \langle p \rangle$ or $\langle b \rangle \subset \langle p \rangle$

$\Rightarrow p \mid a$ or $p \mid b$

$\Rightarrow p$ is a prime in D.

NOTE:- Let D be a PID, and $p \neq 0$ and p is non-unit in D, then the following are equivalent:

(i) p is a prime in D;

(ii) p is irreducible in D;

(iii) $\langle p \rangle$ is a maximal ideal in D;

(iv) $\langle p \rangle$ is a prime ideal in D.

Ex: Let R be a ring with unity. Show that $R[x]/\langle x \rangle \simeq R$.

Define: $f : R[x] \to R$ by $f(a_0 + a_1 x + \cdots + a_n x^n) = a_0$,

$\forall \sum_{i=0}^{n} a_i x^i \in R[x]$; $a_i \in R, \forall i$.

To show that f is well-defined and one-one, let us take $\sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{m} b_i x^i \Leftrightarrow a_0 = b_0$

$\Leftrightarrow f\left(\sum_{i=0}^{n} a_i x^i\right) = f\left(\sum_{i=0}^{m} b_i x^i\right)$. ; $a_i, b_i \in R, \forall i$.

f is onto, since for $a_0 \in R$, $\exists \sum_{i=0}^{n} a_i x^i \in R[x]$ s.t. $f\left(\sum_{i=0}^{n} a_i x^i\right) = a_0$.

$\therefore f$ is a bijection.

To find $\ker f$: Let us consider $f\left(\sum_{i=0}^{n} a_i x^i\right) = 0$

$\Leftrightarrow a_0 = 0 \Leftrightarrow \sum_{i=0}^{n} a_i x^i = x(a_1 + a_2 x + \cdots + a_n x^{n-1}) \in \langle x \rangle$.

$\therefore \ker f = \langle x \rangle$.

To show f is a homomorphism, let us take $\sum_{i=0}^{n} a_i x^i \in R[x]$ and $\sum_{i=0}^{m} b_i x^i \in R[x]$.

$\therefore f\left(\sum_0^n a_i x^i\right) + f\left(\sum_0^m b_i x^i\right) = a_0 + b_0 = f\left(\sum_0^n a_i x^i + \sum_0^m b_i x^i\right)$.

Also, $f\left(\sum_0^n a_i x^i\right) \cdot f\left(\sum_0^m b_i x^i\right) = a_0 \cdot b_0 = f\left[\left(\sum_0^n a_i x^i\right) \cdot \left(\sum_0^m b_i x^i\right)\right]$.

$\therefore$ f is a homomorphism, &

f is a bijection

$\Rightarrow$ f is an isomorphism with $\ker f = \langle x \rangle$.

Thus, by the first law of isomorphism of ring,

$$R[x]/\langle x \rangle \simeq R.$$

Ex. Express the ideal in the I.D. $\mathbb{Z}$ as a principal ideal:
(i) $3\mathbb{Z}+5\mathbb{Z}$, (ii) $8\mathbb{Z}+12\mathbb{Z}$, (iii) $3\mathbb{Z} \cap 5\mathbb{Z}$.

(i) Since every ideal in the I.D. $\mathbb{Z}$ is a principal ideal,

Let $3\mathbb{Z}+5\mathbb{Z} = p\mathbb{Z}$ for some $p \in \mathbb{Z}$.

$\Rightarrow 3\mathbb{Z} \subset p\mathbb{Z}$ and $5\mathbb{Z} \subset p\mathbb{Z}$.

$\Rightarrow p|3$; $\Rightarrow p|5$; Hence p is a common divisor of 3,5.

Let d be any other common divisor of 3, 5.

$\Rightarrow d|3$ and $d|5$ $\Rightarrow 3\mathbb{Z} \subset d\mathbb{Z}$ and $5\mathbb{Z} \subset d\mathbb{Z}$.

$\Rightarrow 3\mathbb{Z}+5\mathbb{Z} \subset d\mathbb{Z} \Rightarrow p\mathbb{Z} \subset d\mathbb{Z} \Rightarrow d|p \Rightarrow p = \gcd(3,5) = 1$.

$\therefore$ $3\mathbb{Z}+5\mathbb{Z} = p\mathbb{Z} = \mathbb{Z}$ [$\because p=1$].

(ii) Proceed in the similar way of (i),

$p = \gcd(8,12) = 4$

$\therefore$ $8\mathbb{Z}+12\mathbb{Z} = p\mathbb{Z} = 4\mathbb{Z}$.

(iii) Let $p\mathbb{Z} = 3\mathbb{Z} \cap 5\mathbb{Z}$, which is a principal ideal in $\mathbb{Z}$.

$\Rightarrow p\mathbb{Z} \subset 3\mathbb{Z}$ and $p\mathbb{Z} \subset 5\mathbb{Z}$.

$\Rightarrow 3|p$ and $5|p \Rightarrow p$ is a common multiple of 3,5.

Let m be any other common multiple of 3,5.

Then $3|m$ and $5|m$

$\Rightarrow m\mathbb{Z} \subset 3\mathbb{Z}$ and $m\mathbb{Z} \subset 5\mathbb{Z}$

$\Rightarrow m\mathbb{Z} \subset 3\mathbb{Z} \cap 5\mathbb{Z} \Rightarrow m\mathbb{Z} \subset p\mathbb{Z} \Rightarrow p|m$

$\Rightarrow p =$ l.c.m of $3, 5 = 15$

$\therefore$ $3\mathbb{Z} \cap 5\mathbb{Z} = p\mathbb{Z} = 15\mathbb{Z}$.

Theorem: Every PID is a UFD.

Proof: Existence of a factorisation:

Let D be a PID and $a \in D$ s.t. $a \neq 0$ and a is non-unit.
If a is irreducible, then D becomes a UFD.
If a is not irreducible, then there exists a factorisation $a = a_1 b_1$, where neither a_1 nor b_1 is a unit.
Hence, $\langle a \rangle \subset \langle a_1 \rangle$.
Now we claim that $\langle a \rangle \neq \langle a_1 \rangle$; otherwise, a and a_1 would be associates and so b_1 would be a unit, a contradiction on our assumption.
Now suppose that $a_1 = a_2 b_2$, where neither a_2 nor b_2 is a unit. By the same argument as before, $\langle a_1 \rangle \subset \langle a_2 \rangle$. We can continue with this construction to obtain an ascending chain of ideals; for this we use the following

Lemma: Let D be a PID. Let $I_1, I_2, \ldots$ be a set of ideals such that $I_1 \subset I_2 \subset \ldots$. Then there exists an integer N such that $I_n = I_N$ for all $n \geq N$. [Proof of this lemma is given below].

By the above lemma, $\exists$ a +ve integer N s.t. $\langle a_n \rangle = \langle a_N \rangle$ for all $n \geq N$. Consequently a_N must be irreducible. Therefore, we conclude that a is the product of two elements, one of which must be irreducible.
Now suppose that $a = c_1 p_1$, where p_1 is irreducible.
If c_1 is not a unit, we can repeat the preceding argument to conclude that $\langle a \rangle \subset \langle c_1 \rangle$.
Either c_1 is irreducible or $c_1 = c_2 p_2$, where p_2 is irreducible and c_2 is not a unit.
Continuing in this manner, we obtain another chain of ideals $\langle a \rangle \subset \langle c_1 \rangle \subset \langle c_2 \rangle \subset \ldots$.
This chain must satisfy the ascending chain condition; therefore, $a = p_1 p_2 \cdots p_r$ for irreducible elements $p_1, p_2, \ldots, p_r$.

Uniqueness of the factorisation:

Let $a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$, where each p_i and each q_i is irreducible.
Without loss of generality, we can assume that $r \leq s$.
Since $p_1 \mid q_1 q_2 \cdots q_s$, it must divide some q_i.
By rearranging the q_i's, we can assume that $p_1 \mid q_1$; hence $q_1 = u_1 p_1$ for some unit $u_1 \in D$.

$\therefore a = p_1 p_2 \cdots p_r = u_1 p_1 q_2 \cdots q_s$

$\Rightarrow p_1 \{(p_2 \cdots p_r) - (u_1 q_2 \cdots q_s)\} = 0$

Since $p_1 \neq 0$, and D is a I.D., hence

$$p_2 \cdots p_r = u_1 q_2 \cdots q_s .$$

Continuing in this manner, we can arrange the q_i's s.t. $p_2 = q_2, p_3 = q_3, \cdots, p_r = q_r$, to obtain $u_1 u_2 \cdots u_r q_{r+1} \cdots q_s = 1$

Here $q_{r+1} \cdots q_s$ is a unit, which contradicts the fact that $q_{r+1}, \cdots, q_s$ are irreducibles.
$\therefore r = s$, and the factorisation of a is unique.

Cor.:- Let F be field, then $F[x]$ is a UFD.

Proof:- If F is a field, then $F[x]$ is an I.D.
Now every ideal in $F[x]$ is a principal ideal, because, if U be any ideal of $F[x]$, then
if $U = \{0\} = \langle 0 \rangle \Rightarrow U$ is a principal ideal, and
if $U \neq \{0\}$, let us suppose that $p(x) \in U$ be a non-zero element of minimal degree.
Now if $\deg(p(x)) = 0$, then $p(x)$ is a non-zero constant polynomial and $1 \in U$. $\langle 1 \rangle = U = F[x]$, [I
$\Rightarrow U$ is again a principal ideal.
Let us now assume that $\deg(p(x)) \geq 1$, and let $f(x) \in U$. Then by Division algorithm for polynomials in $F[x]$, there exist $q(x), r(x) \in F[x]$ s.t. $f(x) = p(x) \cdot q(x) + r(x)$, where either $r(x) = 0$, or $\deg(r(x)) < \deg(p(x))$.
Since U is an ideal and $p(x), f(x) \in U$, and $q(x) \in F[x]$ so that $r(x) = f(x) - p(x) \cdot q(x) \in U$.
Since we choose $p(x)$ to be of minimal degree, $r(x) = 0$. [$\because \deg(r(x)) \not< \deg(p(x))$]
$\therefore f(x) = p(x) \cdot q(x) \Rightarrow U = \langle f(x) \rangle$; $f(x) \in U$ be any element
$\therefore U$ is a principal ideal of $F[x]$.
Since U is any arbitrary ideal of $F[x]$, it follows that every ideal in $F[x]$ is a principal ideal.
$\therefore F[x]$ is a PID.
Since every PID is a UFD, it follows that —
$F[x]$ is a UFD, if F be a field.

REMARKS: Every PID is a UFD, but <u>NOT</u> every UFD is a PID.

Example: $\mathbb{Z}[x]$ is a UFD, but
$\mathbb{Z}[x]$ is NOT a PID.
Because, $\mathbb{Z}$ is a UFD by the Fundamental theorem of Arithmetic $\Rightarrow \mathbb{Z}[x]$ is also a UFD.

So, The ring $\mathbb{Z}[x]$ is an UFD, but NOT a PID.

Let us consider the ideal S of $\mathbb{Z}[x]$ generated by the elements 5 and x of $\mathbb{Z}[x]$.

Then $S = 5f(x) + xg(x)$; $f(x), g(x) \in \mathbb{Z}[x]$.

Let S be a principal ideal of $\mathbb{Z}[x]$, say, $S = \langle h(x) \rangle$ for some $h(x) \in \mathbb{Z}[x]$.

$5 \in S \Rightarrow 5 \in \langle h(x) \rangle \Rightarrow 5 = h(x) \cdot h_1(x)$ for some $h_1(x) \in \mathbb{Z}[x]$

$x \in S \Rightarrow x \in \langle h(x) \rangle \Rightarrow x = h(x) \cdot h_2(x)$ " " $h_2(x)$ "

$\therefore 5h_2(x) = x h_1(x) \Rightarrow$ each coefficient of $h_1(x)$ is a multiple of 5.

$\Rightarrow h_1(x) = 5p(x)$ for some $p(x) \in \mathbb{Z}[x]$.

$\therefore 5 = h(x) \cdot h_1(x) = 5h(x) \cdot p(x)$.

$\Rightarrow h(x) \cdot p(x) = 1$. $\Rightarrow 1 \in \langle h(x) \rangle \Rightarrow 1 \in S$.

$1 \in S \Rightarrow 1 = 5q(x) + xr(x)$ for some $q(x), r(x) \in \mathbb{Z}[x]$

Let $q(x) = a_0 + a_1x + a_2x^2 + \cdots$; $r(x) = b_0 + b_1x + b_2x^2 + \cdots$

Then $1 = 5(a_0 + a_1x + a_2x^2 + \cdots) + x(b_0 + b_1x + b_2x^2 + \cdots)$

$\Rightarrow 5a_0 = 1$, which is an impossibility, since $a_0 \in \mathbb{Z}$.

$\therefore S$ is NOT a principal ideal of $\mathbb{Z}[x]$.

$\therefore$ $\mathbb{Z}[x]$ is NOT a PID.

NOTE: $\mathbb{Z}$ is a UFD $\Rightarrow \mathbb{Z}[x]$ is also a UFD.
BUT $\mathbb{Z}[x]$ is NOT a PID.

So, Every PID is a UFD, BUT the Converse is NOT TRUE.

Give an example to show that — NOT EVERY I.D. IS A UFD.

The subring $\mathbb{Z}[\sqrt{3}i] = \{a + b\sqrt{3}i : a, b \in \mathbb{Z}\}$ of the Complex number $\mathbb{C}$ is an I.D.

Let $z = a + b\sqrt{3}i \in \mathbb{Z}[\sqrt{3}i]$.

Let us define a norm function $N : \mathbb{Z}[\sqrt{3}i] \to \mathbb{N} \cup \{0\}$ by $N(z) = z \cdot \bar{z} = |z|^2 = a^2 + 3b^2$.

$\therefore N(z) \geq 0 \ \forall \ z \in \mathbb{Z}[\sqrt{3}i]$, and $N(z) = 0$ iff $z = 0$.

Also $N(z \cdot w) = N((a+b\sqrt{3}i)\cdot(c+d\sqrt{3}i))$, where $w = c+di \in \mathbb{Z}[\sqrt{3}i]$

$$= N((ac-3bd) + (bc+ad)\sqrt{3}i)$$
$$= (ac-3bd)^2 + 3(bc+ad)^2$$
$$= a^2c^2 + 9b^2d^2 - 6abcd + 3b^2c^2 + 3a^2d^2 + 6abcd$$
$$= a^2(c^2+3d^2) + 3b^2(c^2+3d^2)$$
$$= (a^2+3b^2)\cdot(c^2+3d^2) = N(z)\cdot N(w).$$

$\therefore$ N satisfies all the conditions of Norm function.

If z be a unit in $\mathbb{Z}[\sqrt{3}i]$, $N(z) = 1$, then $a^2 + 3b^2 = 1 \Rightarrow a = \pm 1, b = 0$.

$\Rightarrow z = \pm 1$ are the only units of $\mathbb{Z}[\sqrt{3}i]$

We assert that $4 \in \mathbb{Z}[\sqrt{3}i]$ has following two distinct factorizations into irreducibles in order $\mathbb{Z}[\sqrt{3}i]$ to be a UFD.

$$4 = 2\cdot 2 = (1-\sqrt{3}i)(1+\sqrt{3}i).$$

We must show that each of $2, 1-\sqrt{3}i, 1+\sqrt{3}i$ are irreducible elements in $\mathbb{Z}[\sqrt{3}i]$.

Also 2 is neither associate of $1-\sqrt{3}i$ nor associate of $1+\sqrt{3}i$.

To show 2 is irreducible, let $2 = z\cdot w$

$\therefore N(2) = N(z\cdot w) \Rightarrow 2^2 = N(z)\cdot N(w) = (a^2+3b^2)\cdot(c^2+3d^2)$

$\Rightarrow$ either $a^2+3b^2 = 1, c^2+3d^2 = 4$; or, $a^2+3b^2 = 4, c^2+3d^2 = 1$;

or $a^2+3b^2 = 2, c^2+3d^2 = 2$ [This case does not happen]

Now $a^2+3b^2 = 1 \Rightarrow a = \pm 1, b = 0 \Rightarrow z = a+b\sqrt{3}i = \pm 1$.

and $c^2+3d^2 = 1 \Rightarrow c = \pm 1, d = 0 \Rightarrow w = c+d\sqrt{3}i = \pm 1$.

$\therefore$ when $2 = z\cdot w$, either z or w is a unit

$\Rightarrow$ 2 is irreducible.

Similarly, we can show that $1-\sqrt{3}i, 1+\sqrt{3}i$ are also irreducible.

Since 1 and -1 are only units, and $2 \neq \pm 1(1 \pm \sqrt{3}i)$

$\therefore$ 2 is associate of neither $1+\sqrt{3}i$ nor $1-\sqrt{3}i$.

THEOREM: If D is a UFD, then $D[x]$ is a UFD.

PROOF: Let $p(x)$ be a non-zero polynomial in $D[x]$. If $p(x)$ is a constant polynomial, then it must have a unique factorization since D is a UFD. Now let us suppose that $p(x)$ is a polynomial of positive degree in $D[x]$.

Let F be the field of fractions of D, and let $p(x) = f_1(x) f_2(x) \cdots f_n(x)$ by a factorization of $p(x)$, where each $f_i(x)$ is irreducible.

Let us choose $a_i \in D$ such that $a_i f_i(x) \in D[x]$.

There exist $b_1, b_2, \cdots, b_n \in D$ such that $a_i f_i(x) = b_i g_i(x)$, where $g_i(x)$ is a primitive polynomial in $D[x]$, and each $g_i(x)$ is irreducible in $D[x]$.

Consequently, we can write

$$a_1 \cdots a_n p(x) = b_1 \cdots b_n g_1(x) \cdots g_n(x).$$

Let $b_1 \cdots b_n = b$. Since $g_1(x) \cdots g_n(x)$ is primitive, $a_1 \cdots a_n$ divides b.

$\therefore p(x) = a g_1(x) \cdots g_n(x)$, where $a \in D$.

Since D is a UFD, we can factor a as $u c_1 \cdots c_k$, where u is a unit and each c_i's is irreducible in D.

To show Uniqueness of this factorization:

Let $p(x) = a_1 \cdots a_m f_1(x) \cdots f_n(x) = b_1 \cdots b_r g_1(x) \cdots g_s(x)$ be two factorizations of $p(x)$, where all of the factors are irreducible in $D[x]$. And each of the f_i's and g_i's is irreducible in $F[x]$.

The a_i's and the b_i's are units in F.

Since $F[x]$ is a PID, it is a UFD; therefore, $n = s$.

Now re-arrange the $g_i(x)$'s so that $f_i(x)$ and $g_i(x)$ are associates for $i = 1, 2, \cdots, n$.

EUCLIDEAN DOMAIN.

When a division algorithm is available for an I.D. ??

Definition → An I.D. D is said to be a Euclidean domain if there exists a function $v : D-\{0\} \to \mathbb{Z}^+ \cup \{0\}$ satisfying the following conditions —

1. $v(a) \leq v(ab)$, $\forall\ a(\neq 0), b(\neq 0)$ in D; and
2. $\forall\ a, b \in D$ with $b \neq 0$, there exist q, r in D s.t. $a = b \cdot q + r$, where either $r = 0$ or $v(r) < v(b)$.

The function v is called a Euclidean valuation on D.

Examples:—

① $\mathbb{Z}$ is a Euclidean domain (E.D.)

Let us define a function v on $\mathbb{Z}$ by
$v(a) = |a|$, $\forall\ a(\neq 0) \in \mathbb{Z}$.
Let $a(\neq 0), b(\neq 0)$ in $\mathbb{Z}$. Then $a.b \in \mathbb{Z}$ and $a.b \neq 0$, since $\mathbb{Z}$ is an I.D., & contains no zero divisor.
$\therefore v(a.b) = |a.b| = |a| \cdot |b| = v(a) \cdot v(b)$
Since $v(b) > 0$, we have $v(a) \leq v(a.b)$ ——→ ①
Let $a, b \in \mathbb{Z}$ and $b \neq 0$. By Division algorithm, $\exists$ integers q and r s.t. $a = b.q + r$; either $r = 0$ or $0 < r < |b|$.
Now $0 < r < |b| \Rightarrow |r| < |b| \Rightarrow v(r) < v(b)$. ——→ ②
Thus v satisfies both the conditions of a Euclidean valuation on $\mathbb{Z}$. Thus $\mathbb{Z}$ is a E.D.

② A field F is a E.D.

Let us define a function v on F by
$v(a) = I$, $\forall\ a(\neq 0)$ in F, I being the unity in F.
Let $a(\neq 0), b(\neq 0)$ in F, then $a.b \neq 0$ in F, as F is an I.D., & F contains no zero divisor.
Now $v(a.b) = I = I.I = v(a) \cdot v(b) \Rightarrow v(a) \leq v(a.b)$.
Let $a, b \in F$ and $b \neq 0$. Then $b^{-1} \in F$ and
$a = (bb^{-1}).a = b.(b^{-1}a) + 0 = b.q + r$, where $q = b^{-1}a \in F$ and $r = 0 \in F$. Thus v is a Euclidean valuation on F.

③ If F be a field, then $F[x]$ is a E.D.

Let us define a function v on $F[x]$ by

$v(f(x)) = \deg(f(x))$; $\forall\, f(x)(\neq 0)$ in $F[x]$.

$\because v(f(x)) \geq 0$, $\forall\, f(x) \neq 0$ in $F[x]$.

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

Then $v(f(x)\cdot g(x)) = \deg(f(x)\cdot g(x)) = \deg(f(x)) + \deg(g(x)) \geq \deg(f(x))$.

$\therefore v(f(x)\cdot g(x)) \geq v(f(x))$; Since $F[\,]$ is an I.D.

$\therefore v(f(x)) \leq v(f(x)\cdot g(x))$, $\forall\, f(x)\neq 0, g(x)\neq 0$ in $F[x]$

Let $f(x), g(x)$ be in $F[x]$ and $g(x)\neq 0$, then by division algorithm for polynomials, $\exists$ unique polynomials $q(x), r(x)$ in $F[x]$ s.t.

$f(x) = q(x)\cdot g(x) + r(x)$; where either $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$ i.e., $v(r(x)) < v(g(x))$.

$\therefore v$ satisfies both the conditions of a Euclidean valuation on $F[x]$.

$\therefore F[x]$ becomes a E.D.

④ $\mathbb{Z}[i]$, the set of Gaussian integers, is a E.D.

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

Let us define a function v on $\mathbb{Z}[i]$ by

$v(a+bi) = |a+bi|^2 = a^2+b^2$, $\forall\, a+bi(\neq 0)$ in $\mathbb{Z}[i]$.

Let $z, w \in \mathbb{Z}[i]$ s.t. $z\neq 0$, $w\neq 0$, then $z.w\neq 0$,

$v(z.w) = |z.w|^2 = |z|^2|w|^2 = v(z)\cdot v(w)$

$\Rightarrow v(z) \leq v(z\cdot w)$, since $v(w) > 0$

Next to show: for $z, w \in \mathbb{Z}[i]$ with $w\neq 0$, $\exists\, q, r \in \mathbb{Z}[i]$ s.t. $z = q\cdot w + r$, either $r = 0$ or $v(r) < v(w)$.

For, $z.w^{-1} = (a+bi)\cdot(c+di)^{-1}$, where $z = a+bi$, $w = c+di$; $a, b, c, d \in \mathbb{Z}$.

$$= \frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}\,i$$

$$= \left(m_1 + \frac{n_1}{c^2+d^2}\right) + \left(m_2 + \frac{n_2}{c^2+d^2}\right)i, \text{ say.}$$

$$= (m_1 + m_2 i) + \left(\frac{n_1}{c^2+d^2} + \frac{n_2}{c^2+d^2}\,i\right)$$

$$= \underbrace{(m_1 + m_2 i)}_{\text{integer part}} + \underbrace{(s+ti)}_{\text{proper fraction}} \in \mathbb{Q}[i] = \{p+qi : p, q \in \mathbb{Q}\}$$

We take the closest integers m_1, m_2 s.t. the fractional parts $s(=\frac{n_1}{c^2+d^2})$ and $t(=\frac{n_2}{c^2+d^2})$ satisfy $|s| \le \frac{1}{2}$, $|t| \le \frac{1}{2}$.

Now $z = z(\omega^{-1}\omega) = \omega(z\omega^{-1}) = \omega(m_1+m_2 i)+\omega(s+ti)$

$\therefore z = q\cdot\omega + r$, where

$q = m_1+m_2 i \in \mathbb{Z}[i]$, $r = \omega(s+ti) \in \mathbb{Z}[i]$.

$\therefore v(r) = v(\omega)\cdot v(s+ti) \le v(\omega)\cdot\frac{1}{2}$ [$\because v(s+ti) = s^2+t^2 \le \frac{1}{4}+\frac{1}{4} = \frac{1}{2}$]

$\therefore v(r) < v(\omega)$.

$\therefore \mathbb{Z}[i]$ is a E.D. with a Euclidean valuation v defined on $\mathbb{Z}[i]$.

Th. Every E.D. is a PID.

Proof: Let D be a E.D. and v be a Euclidean valuation on D.

Let U be an ideal in D.

Case 1. If U is trivial ideal, then $U = \{0\} = \langle 0\rangle$.
$\therefore U$ is a principal ideal and D becomes a PID.

Case 2. If U is non-trivial ideal, then let us choose $b(\neq 0) \in U$ s.t. $v(b)$ is minimal of all $v(x)$ for non-zero x in U. Such b exists by the well-ordering property of $\mathbb{N}$.

Let $a \in U$, then by the property of the Euclidean valuation v, $\exists$ elements q and r in D s.t.
$a = b\cdot q + r$, where either $r = 0$ or $v(r) < v(b)$.
Since U is an ideal, $a \in U$, $b \in U$ and $q \in D$
$\Rightarrow r = a - b\cdot q \in U$.
Now $v(r) < v(b)$ is not possible because
$v(b) < v(x)$, $\forall\, x(\neq 0) \in U$.
$\therefore r = 0 \Rightarrow a = b\cdot q$ for some $q \in D$.
Since $a \in U$, is an arbitrary element,
$\therefore U = \langle b\rangle$, a principal ideal.
$\therefore$ Every ideal in a E.D. is a principal ideal
$\Rightarrow$ Every E.D. is a PID.

NOTE :- ① A PID is a UFD, and a E.D. is a PID
$\Rightarrow$ A E.D. is a UFD.

② A PID may not be a E.D.

③ In a E.D. any two non-zero elements a and b have a gcd; if $d = \gcd(a,b)$, then $d = a \cdot u + b \cdot v$ for some $u, v \in D$.

④ In a E.D. any two non-zero elements a, b have a lcm.

Euclidean Algorithm :-

Let $a(\neq 0), b(\neq 0)$ be in E.D. D with $v(a) \geq v(b)$.
Then $\exists\ q_1, r_1 \in D$ s.t. $a = b \cdot q_1 + r_1$, where either $r_1 = 0$, or $v(r_1) < v(b)$.

If $r_1 = 0$, then $\gcd(a,b) = b$.

If $r_1 \neq 0$, " $\exists\ q_2, r_2 \in D$ s.t. $b = q_2 r_1 + r_2$, where either $r_2 = 0$ or $v(r_2) < v(r_1)$.

If $r_2 = 0$, then $b = q_2 \cdot r_1 \Rightarrow r_1 | b \Rightarrow r_1 | a$ [$\because a = b \cdot q_1 + r_1$]

$\therefore$ $r_1 | a$ and $r_1 | b$.

Let $c|a, c|b \Rightarrow c|(a - b \cdot q) \Rightarrow c|r_1$

$\Rightarrow r_1 = \gcd(a,b)$.

If $r_2 \neq 0$, we proceed in a similar manner.
The process continues until remainder becomes zero.
And the last non-zero remainder is the $\gcd(a,b)$.

$\gcd(a,b) = a \cdot u + b \cdot v$; $u, v \in D$.