Principal Ideal Domains [PID].

Let R be a commutative ring with identity.
A principal ideal generated by $a \in R$ is an ideal $\langle a \rangle = \{ra : r \in R\}$.

Definition → An I.D. in which every ideal is principal is called 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 of F are $\{0\}$ and F itself.
   $\{0\}$ is the principal ideal $\langle 0 \rangle$, and
   F " " " " $\langle 1 \rangle$.

Lemma: Let D be an I.D. and let $a, b \in D$. Then

(i) $b \mid a$ if and only if $\langle a \rangle \subset \langle b \rangle$
(ii) a and b are associates if and only if $\langle a \rangle = \langle b \rangle$
(iii) a is a unit in D if and only if $\langle a \rangle = D$.

Proof:

(i) Suppose that $b \mid a$. Then $a = b.x$ for some $x \in D$.
Hence, for every $r \in D$, $ar = (bx)r = b.(xr)$
$\Rightarrow \langle a \rangle \subset \langle b \rangle$
Conversely, let $\langle a \rangle \subset \langle b \rangle$. Then $a \in \langle b \rangle$ [$\because a \in \langle a \rangle$]
$\Rightarrow a = b.x$ for some $x \in D$.
$\Rightarrow b \mid a$.

(ii) Since a and b are associates, $a \mid b$ and $b \mid a$.
Now by (i), $a \mid b \Rightarrow \langle b \rangle \subset \langle a \rangle$ and $b \mid a \Rightarrow \langle a \rangle \subset \langle b \rangle$ $\Big\} \Rightarrow \langle a \rangle = \langle b \rangle$.
Conversely, let $\langle a \rangle = \langle b \rangle$. Then $\langle a \rangle \subset \langle b \rangle \Rightarrow b \mid a$,
and $\langle b \rangle \subset \langle a \rangle \Rightarrow a \mid b$.
$\therefore$ a and b are associates.

(iii) An element $a \in D$ is a unit if and only if a is an associate of 1.
However, a is an associate of 1 if and only if $\langle a \rangle = \langle 1 \rangle = D$ [by (ii)].

Theorem: Let D be a PID and $\langle p \rangle$ be a non zero ideal in D. Then $\langle p \rangle$ is a maximal ideal if and only if p is irreducible.

Proof:- Suppose that $\langle p \rangle$ is a maximal ideal.
If some $a \in D$ divides p, then $\langle p \rangle \subset \langle a \rangle$.
Since $\langle p \rangle$ is maximal, either $D = \langle a \rangle$ or $\langle p \rangle = \langle a \rangle$.
Consequently, either a is a unit or a and p are associates.
$\therefore$ p is irreducible.

Conversely, let p be irreducible.
If $\langle a \rangle$ is an ideal in D s.t. $\langle p \rangle \subset \langle a \rangle \subset D$, then $a \mid p$.
Since p is irreducible, either a is a unit, or a and p are associates.
$\therefore$ either $D = \langle a \rangle$ or $\langle p \rangle = \langle a \rangle$.
Thus, $\langle p \rangle$ is a maximal ideal.

Corollary: Let D be a PID. If p is irreducible, then p is prime.

Proof: Let p be irreducible and suppose that $p \mid ab$. Then $\langle ab \rangle \subset \langle p \rangle$.
Since p is irreducible, then by previous theorem, $\langle p \rangle$ is a maximal ideal.
We know that every maximal ideal in a commutative ring with identity is also a prime ideal.
$\therefore$ $\langle p \rangle$ must be a prime ideal.
Thus, $ab \in \langle p \rangle \Rightarrow$ either $a \in \langle p \rangle$ or $b \in \langle p \rangle$.
$\Rightarrow$ either $p \mid a$ or $p \mid b$
$\therefore$ 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.

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 $I_1 \subset I_2 \subset \cdots$. 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 $\langle a \rangle \subset \langle c_1 \rangle \subset \langle c_2 \rangle \subset \cdots$.
This chain must satisfy the ascending chain condition; therefore, $a = p_1 p_2 \cdots p_n$ for irreducible elements $p_1, p_2, \ldots, p_n$.

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 $r < s$.

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.

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

Proof: If F is a field, then $F[x]$ is an I.D..

Also every ideal in $F[x]$ is a principal ideal. (Proof) Hence $F[x]$ is a PID.

We have proved that every PID is a UFD.

Therefore, $F[x]$ is a UFD.

Proof of: Every ideal in $F[x]$ is a principal ideal.

Let F be a field. Then a principal ideal in $F[x]$ is an ideal $\langle p(x) \rangle = \{ p(x) \cdot q(x) : q(x) \in F[x] \}$.

Now suppose that U be an ideal of $F[x]$. If U is the

zero ideal, then it is true.
Suppose that U is a non-trivial ideal in $F[x]$, and let $p(x) \in U$ be a non-zero element of minimal degree.
If $\deg p(x) = 0$, then $p(x)$ is a non zero constant polynomial and $1 \in U$.
Since 1 generates all of $F[x]$, $\langle 1 \rangle = U = F[x]$ and U is again a principal ideal.
Now let us assume that $\deg p(x) \geq 1$ and let $f(x) \in U$. Then by the division algorithm there exist $q(x), r(x)$ in $F[x]$ s.t
$f(x) = p(x)\,q(x) + r(x)$, where either $r(x) = 0$, or $\deg(r(x)) < \deg(p(x))$.
Since $f(x), p(x) \in U$ and U is an ideal,
$r(x) = f(x) - p(x) \cdot q(x) \in U$.
However, since we choose $p(x)$ to be of minimal degree, $r(x)$ must be the zero polynomial.
$\therefore f(x) = p(x) \cdot q(x)$ for some $q(x) \in F[x]$.
where $f(x) \in U$ is any element.
$\therefore U = \langle p(x) \rangle$.
$\therefore$ Every ideal in $F[x]$ is a principal ideal.

Remark: Every PID is a UFD, but not every UFD is a PID.

Example → Let us consider the polynomial ring $\mathbb{Z}[x]$. The set $\mathbb{Z}$ is a UFD by the fundamental theorem of Arithmetic.
Again we know if $\mathbb{Z}$ is a UFD, then $\mathbb{Z}[x]$ is also a UFD.
However, $\mathbb{Z}[x]$ is not a PID. To prove this, let $U = \{5f(x) + x\,g(x) : f(x), g(x) \in \mathbb{Z}[x]\}$.
It can easily be shown that U is an ideal of $\mathbb{Z}[x]$.
Let $U = \langle p(x) \rangle$. Since $5 \in U$, $5 = f(x) \cdot p(x)$. In this case $p(x) = p$ must be constant. Since $x \in U$, $x = pg(x)$;
Consequently, $p = \pm 1$. However, $\langle p(x) \rangle = \mathbb{Z}[x]$.
This would mean that $3 \in U$. So we can write
$3 = 5f(x) + x\,g(x) \Rightarrow 3 = 5f(x)$, which is impossible.
(constant term)

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 numbers $\mathbb{C}$ is an I.D.

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

$\alpha(z) \geq 0$ and $\alpha(z) = 0$ when $z = 0$. Also

$\alpha(zw) = \alpha(z)\alpha(w)$.

If $\alpha(z) = 1$, then $a^2 + 3b^2 = 1 \Rightarrow z$ is a unit.

Only units of $\mathbb{Z}[\sqrt{3}i]$ are 1 and -1.

We assert that 4 has two distinct factorizations into irreducible elements:

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

We must show that each of these factors is an irreducible element in $\mathbb{Z}[\sqrt{3}i]$.

If 2 is not irreducible, then $2 = zw$ for $z, w \in \mathbb{Z}[\sqrt{3}i]$ where $\alpha(z) = \alpha(w) = 2$.

Now $\alpha(z) = 2 \Rightarrow a^2 + 3b^2 = 2$ has no integer solutions. $\Rightarrow$ 2 must be irreducible.

Similarly both $1 - \sqrt{3}i$ and $1 + \sqrt{3}i$ are irreducible, because, if $1 - \sqrt{3}i = zw$ for $z, w \in \mathbb{Z}[\sqrt{3}i]$ where $\alpha(z) = \alpha(w) = 1 - \sqrt{3}i$

$\Rightarrow a^2 + 3b^2 = 1 - \sqrt{3}i$ has no integer solutions.

Since 2 is not a unit multiple of either $1 - \sqrt{3}i$ or $1 + \sqrt{3}i$, 4 has at least two distinct factorizations into irreducible elements.

Euclidean Domain

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

Definition: Let D be an I.D. such that for each $a \in D$ there is a non-negative integer $v(a)$ satisfying the following conditions.

1. If a and b are non zero elements in D, then $v(a) \leq v(ab)$.
2. Let $a, b \in D$ with $b \neq 0$. Then there exist elements q and $r \in D$ such that $a = bq + r$, where either $r = 0$ or $v(r) < v(b)$.

Then D is called a Euclidean domain and v is called a Euclidean valuation.

Remarks: $v : D \to \mathbb{Z}^+$ a function defined on the non-zero elements of D.

Example: ①. The set of Gaussian integers

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

We define $v(a+bi) = |a+ib|^2 = a^2 + b^2$ as a Euclidean valuation on $\mathbb{Z}[i]$.

Let $z, w \in \mathbb{Z}[i]$. Then $v(zw) = |zw|^2 = |z|^2 |w|^2 = v(z)v(w)$.

Since $v(z) \geq 1$ for every non zero $z \in \mathbb{Z}[i]$,

$v(z) \leq v(z)\, v(w) = v(zw)$

Therefore, $v(z) \leq v(zw)$ for $z \neq 0, w \neq 0$ in $\mathbb{Z}[i]$.

Next, we must show that for any $z = a+bi$ and $w = c+di$ in $\mathbb{Z}[i]$ with $w \neq 0$, there exist elements $q, r \in \mathbb{Z}[i]$ s.t. $z = qw + r$, where either $r = 0$ or $v(r) < v(w)$.

Now $zw^{-1} = (a+bi) \cdot \dfrac{c-di}{c^2+d^2} = \dfrac{ac+bd}{c^2+d^2} + \dfrac{bc-ad}{c^2+d^2} i$

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

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

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

We take the closest integer m_i s.t. the fractional part satisfies $|ni/(c^2+d^2)| \leq \frac{1}{2}$.

eg. $\frac{9}{8} = 1 + \frac{1}{8}$; $\frac{15}{8} = 2 - \frac{1}{8}$

Thus, s and t are the "fractional parts" of $z\omega^{-1} = (m_1 + m_2 i) + (s+ti)$, where $|s| \leq \frac{1}{2}, |t| \leq \frac{1}{2}$.

$s^2 + t^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$.

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

where $q = m_1 + m_2 i$ and $r = \omega(s+ti)$.

Since $z \in \mathbb{Z}[i]$ and $q\omega \in \mathbb{Z}[i]$, then $r \in \mathbb{Z}[i]$

Now $v(r) = v(\omega)\, v(s+ti) \leq \frac{1}{2} v(\omega) < v(\omega)$ $\left[\because v(s+ti) = s^2+t^2 \leq \frac{1}{2}\right]$

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

$\therefore$ $\mathbb{Z}[i]$ is a Euclidean domain with a Euclidean valuation defined on $\mathbb{Z}[i]$ is given by $v(a+bi) = a^2+b^2$.

Example: ②. Let F be a field. Then the degree of a polynomial in $F[x]$ is a Euclidean valuation.

Let us define $v(f(x)) = \deg(f(x))$ for $f(x) \neq 0$ in $F[x]$.

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

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

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

$\therefore$ $v(f(x)) \leq v(f(x)\cdot g(x))$.

If $f(x), g(x) \in F[x]$ with $g(x) \neq 0$, then by division algorithm $\exists$ unique polynomials $q(x)$ & $r(x) \in F[x]$ s.t. $f(x) = g(x)\cdot q(x) + r(x)$, where either $r(x) = 0$, or, $\deg(r(x)) < \deg(g(x))$ i.e., $v(r(x)) < v(g(x))$,

$\therefore$ v satisfies all the conditions of Euclidean domain.

$\therefore$ $F[x]$ is an Euclidean domain with v as defined above.

Theorem: Every Euclidean domain is a PID.

Proof: Let D be a Euclidean domain and v be a Euclidean valuation on D.
Let us suppose U is a non-trivial ideal in D and let us choose $b(\neq 0) \in U$ s.t. $v(b)$ is minimal for all $a \in U$.
Since D is a Euclidean domain, $\exists$ elements q and r in D s.t. $a = bq + r$, where either $r = 0$ or $v(r) < v(b)$.
But $r = a - bq \in U$, since U is an ideal.
$\therefore r = 0$ by the minimality of b.
$\Rightarrow a = bq \Rightarrow U = \langle b \rangle$
$\therefore U$ is a principal ideal in D.
$\therefore$ Every ideal in a Euclidean domain D is a principal ideal.
So, D is a PID. Hence the theorem.

Corollary: Every Euclidean domain is a UFD.
We have every Euclidean domain is a PID.
Also we have every PID is a UFD.
Therefore the result follows.

Note: Let D be a Euclidean domain with Euclidean valuation v. Then
(i) $v(a) \geq v(1)$ $\forall$ non-zero $a \in D$.
(ii) $u \in D$ is a unit iff $v(u) = v(1)$.

Note: If v be a Euclidean valuation on a Euclidean domain D, then a different Euclidean valuation can also be defined on D.
For example, on the I.D. $\mathbb{Z}$, let us define two functions: v and ω by
$v(a) = |a|$, $\forall$ non-zero $a \in \mathbb{Z}$.
and $\omega(n) = |n| + 2$, $\forall$ " " $n \in \mathbb{Z}$,
Then both v & ω are Euclidean valuation on the I.D. $\mathbb{Z}$.

Th:(1) Let D be a Euclidean domain with Euclidean valuation v. For $a(\neq 0), b(\neq 0)$ in D,
$v(a) < v(ab)$ if and only if b be a non-unit.

(2) If a and b are associates in D, then $v(a)=v(b)$.

(3) If $a|b$ and $v(a)=v(b)$, then a & b are associates.

(4) If a is a proper divisor of b, then $v(a)<v(b)$.
But the converse is not true.

Euclidean Algorithm

Let $a(\neq 0), b(\neq 0)$ be in D with $v(a) \geq v(b)$.
Then there exist elements q_1 and r_1 in D
s.t. $a = bq_1 + r_1$, where either $r_1 = 0$, or $v(r_1) < v(b)$.
If $r_1 = 0$, then $\gcd(a,b) = b$.
If $r_1 \neq 0$, then process continues until remainder becomes zero. And the last non-zero remainder is the $\gcd(a,b)$.
And $\gcd(a,b) = au + bv$, where $u, v \in D$.

Remarks.

Fields $\subset$ Euclidean domains $\subset$ PID $\subset$ UFD $\subset$ I.D.

Ex - 22 / S. K. Mapa / pg - 261.

(1) Find the units in the integral domain $Z[\sqrt{-2}]$.

On the I.D. $Z[\sqrt{-2}]$, for $\alpha \in Z[\sqrt{-2}]$, we define $N(\alpha) = \alpha.\bar{\alpha} = a^2 + 2b^2$; where $\alpha = a + b\sqrt{-2} \in Z[\sqrt{-2}]$, so $\bar{\alpha} = a - b\sqrt{-2}$.

Then $N(\alpha) \geq 0$, $\forall \alpha \in Z[\sqrt{-2}]$ and $N(\alpha) = 0$ iff $\alpha = 0$.

$N(\alpha.\beta) = N(\alpha).N(\beta)$, $\forall \alpha, \beta \in Z\sqrt{-2}$; Because, if $\beta = c + d\sqrt{2}$, then $\alpha.\beta = (a+b\sqrt{-2}).(c+d\sqrt{-2}) = (ac-2bd) + (bc+ad)\sqrt{2}$.

$\therefore N(\alpha.\beta) = (ac-2bd)^2 + 2(bc+ad)^2 = a^2c^2 + 2(b^2c^2 + a^2d^2) + 4b^2d^2$

$N(\alpha).N(\beta) = (a^2+2b^2)(c^2+2d^2) = a^2c^2 + 2(b^2c^2 + a^2d^2) + 4b^2d^2$

$\therefore N(\alpha.\beta) = N(\alpha).N(\beta)$

So, N is a norm function on $Z[\sqrt{-2}]$.

Let $\alpha \in Z[\sqrt{-2}]$ be a unit, then $N(\alpha) = 1 \Rightarrow \alpha.\bar{\alpha} = 1$

$\Rightarrow \alpha$ is a unit, since $\bar{\alpha} \in Z[\sqrt{-2}]$.

$\therefore \alpha$ is a unit iff $N(\alpha) = 1$.

$\Rightarrow a^2 + 2b^2 = 1$ for $a, b \in Z$.

$\Rightarrow a = \pm 1, b = 0$.

Hence the units in the domain $Z[\sqrt{-2}]$ are 1 and -1.

(3) Show that the domain $Z[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in Z\}$ is not a UFD by showing the element 21 has two different factorisations into irreducibles as $21 = 3.7 = (1+2\sqrt{-5})(1-2\sqrt{-5})$.

On the domain $Z[\sqrt{-5}]$, $21 = 3.7 = (1+2\sqrt{-5})(1-2\sqrt{-5})$.

We prove that each of $3, 7, 1+2\sqrt{-5}, 1-2\sqrt{-5}$ is an irreducible in $Z[\sqrt{-5}]$.

Let $3 = (a+b\sqrt{-5})(c+d\sqrt{-5})$. Then $N(3) = N(a+b\sqrt{-5})N(c+d\sqrt{-5})$

$\Rightarrow 9 = (a^2+5b^2)(c^2+5d^2)$ for $a, b, c, d \in Z$.

This is possible, if

either (i) $a^2+5b^2 = 1$ and $c^2+5d^2 = 9$, $\Rightarrow a = \pm 1, b = 0; c = \pm 3, d = 0$

or (ii) $a^2+5b^2 = 3$ and $c^2+5d^2 = 3$, cannot happen

or (iii) $a^2+5b^2 = 9$ and $c^2+5d^2 = 1 \Rightarrow c = \pm 1, d = 0$; $a = \pm 3, b = 0$.

So in (i) $a+b\sqrt{-5}$ is a unit,

and in (iii) $c+d\sqrt{-5}$ " "

$\therefore$ if $3 = (a+b\sqrt{-5})(c+d\sqrt{-5})$ then either $a+b\sqrt{-5}$ is a unit or $c+d\sqrt{-5}$ is a unit.

$\Rightarrow 3$ is an irreducible in $Z[\sqrt{-5}]$.

Similarly 7 is an irreducible in $Z[\sqrt{-5}]$.

To show $1+2\sqrt{-5}$ is an irreducible in $Z[\sqrt{-5}]$,

Let $1+2\sqrt{-5} = (p+q\sqrt{-5})(r+s\sqrt{-5})$, then

$N(1+2\sqrt{-5}) = N(p+q\sqrt{-5})\,N(r+s\sqrt{-5})$

i.e., $1^2 + 2^2(\sqrt{-5})^2 = (p^2+5q^2)(r^2+5s^2)$

i.e., $21 = (p^2+5q^2)(r^2+5s^2)$.

$\Rightarrow$ either (i) $p^2+5q^2 = 1,\ r^2+5s^2 = 21 \Rightarrow p=\pm1, q=0; \{r=\pm1, s=\pm2;\ r=\pm4, s=\pm1\}$

or (ii) $p^2+5q^2 = 21,\ r^2+5s^2 = 1 \Rightarrow \{p=\pm1, q=\pm2;\ p=\pm4, q=\pm1\}; r=\pm1, s=0$.

or (iii) $p^2+5q^2 = 3,\ r^2+5s^2 = 7 \Rightarrow$ It is not possible.

or (iv) $p^2+5q^2 = 7,\ r^2+5s^2 = 3 \Rightarrow$ " " " "

In (i) $p^2+5q^2 = 1 \Rightarrow p=\pm1, q=0$; so $p+q\sqrt{-5}$ is a unit.

In (ii) $r^2+5s^2 = 1 \Rightarrow r=\pm1, s=0$, so $r+s\sqrt{-5}$ " " "

This proves that $1+2\sqrt{-5}$ is an irreducible in $Z[\sqrt{-5}]$.

Similarly $1-2\sqrt{-5}$ " " " " ".

We have two different factorisations of 21 into irreducibles.

None of the factors $1+2\sqrt{-5}$ and $1-2\sqrt{-5}$ is an associate of 3 or 7, since 1 and -1 are the only units in $Z[\sqrt{-5}]$.

So the domain $Z[\sqrt{-5}]$ is not a UFD.

(4) Show that 2 is an irreducible element in the domain $D = Z[\sqrt{-6}]$. Using the equality $2\cdot5 = (2+\sqrt{-6})(2-\sqrt{-6})$, establish that 2 is not a prime element in D. Deduce that D is not a UFD.

Let us define a norm function N on D by

$N(a+b\sqrt{-6}) = a^2+6b^2$.

Let $2 = (a+b\sqrt{-6})(c+d\sqrt{-6})$. Then

$N(2) = N(a+b\sqrt{-6})\cdot N(c+d\sqrt{-6})$ for $a, b, c, d \in Z$.

$\Rightarrow 4 = (a^2+6b^2)(c^2+6d^2) \Rightarrow a=\pm1, b=0; c=\pm2, d=0$

$\Rightarrow$ either (i) $a^2+6b^2 = 1,\ c^2+6d^2 = 4$

or (ii) $a^2+6b^2 = 4,\ c^2+6d^2 = 1 \Rightarrow a=\pm2, b=0; c=\pm1, d=0$.

or (iii) $a^2+6b^2 = 2,\ c^2+6d^2 = 2 \Rightarrow$ This cannot happen

In (i) $a+b\sqrt{-6}$ is a unit, and in (ii) $c+d\sqrt{-6}$ is a unit.

Therefore, if $2 = (a+b\sqrt{-6})(c+d\sqrt{-6})$, then either $a+b\sqrt{-6}$ is a unit or $c+d\sqrt{-6}$ is a unit,

$\therefore$ 2 is an irreducible in D.

Using the equality $2 \cdot 5 = (2+\sqrt{-6})(2-\sqrt{-6})$ in the I.D. $D = \mathbb{Z}[\sqrt{-6}]$, we proved that 2 is irreducible, and $2 \mid (2+\sqrt{-6})(2-\sqrt{-6})$.

But $2 \nmid (2+\sqrt{-6})$ and $2 \nmid (2-\sqrt{-6})$

i.e., 2 is neither a divisor of $2+\sqrt{6}$ nor a divisor of $2-\sqrt{-6}$.

So 2 is not a prime in $D = \mathbb{Z}[\sqrt{-6}]$.

Now to show that D is not a UFD.

We have prove that 2 is an irreducible in D

Similarly we can show that 5, $2+\sqrt{-6}$, $2-\sqrt{-6}$ are also irreducibles in D.

From $10 = 2 \cdot 5 = (2+\sqrt{-6}) \cdot (2-\sqrt{-6})$, we have two different factorisations of 10 into irreducibles.

None of the factors $2+\sqrt{-6}$ and $2-\sqrt{-6}$ is an associate of 2 or 5, since 1 and -1 are the only units in D.

So the domain $D = \mathbb{Z}[\sqrt{-6}]$ is not a UFD.

⑤ Show that the elements 21 and $3(1+2\sqrt{-5})$ in the domain $\mathbb{Z}[\sqrt{-5}]$ have no gcd. Deduce that the domain is not a UFD.

Let $\alpha = 21 = 3 \cdot 7 = (1+2\sqrt{-5})(1-2\sqrt{-5})$, $\beta = 3(1+2\sqrt{-5})$

Let us define a norm function N on $\mathbb{Z}[\sqrt{-5}]$ by $N(a+b\sqrt{-5}) = a^2+5b^2$.

3 is a common divisor of α and β.

$1+2\sqrt{-5}$ " " " α " β

Let $\gamma = 3$, $\delta = 1+2\sqrt{-5}$.

Let $d = a+b\sqrt{-5}$ be a gcd of α and β.

Then $N(d)$ is a common divisor of $N(\alpha)$ and $N(\beta)$

i.e, $N(d)$ " " " " " 441 and 189

∴ possible values of $N(d)$ are 1, 3, 7, 9, 21, 63.

Since $d = \gcd(\alpha, \beta)$ & γ is a common divisor of α, β, $N(\gamma) \mid N(d)$. Similarly $N(\delta) \mid N(d)$. But $N(\gamma) = 9$, $N(\delta) = 21$.

∴ $N(d)$ must be 63. Then $a^2+5b^2 = 63$.

No integers a, b can be found to satisfy $a^2+5b^2=63$.

$\therefore$ there is no element in $Z[\sqrt{-5}]$ that may be a gcd of α and β.

Since any two elements 21 and $3(1+2\sqrt{-5})$ in $Z[\sqrt{-5}]$ have no gcd, it follows that the domain $Z[\sqrt{-5}]$ is not a UFD, since in a UFD, any two non-zero elements have a gcd.

(6) For an element $\alpha = a+bi$ in the domain $Z[i]$, a^2+b^2 is a prime integer. Prove that α is an irreducible element in the domain. Show that the elements are irreducible in the domain $Z[i]$: (ii) $2+3i$.

We define a norm function N on the domain $Z[i]$ by $N(\alpha) = N(a+bi) = a^2+b^2 = p$, say.

Let $\alpha = \beta\gamma \Rightarrow N(\alpha) = N(\beta)\cdot N(\gamma)$

$\Rightarrow p = N(\beta)\cdot N(\gamma)$

Since p is a prime, either $N(\beta)=1$ or $N(\gamma)=1$.

i.e., either β is a unit, or γ is a unit.

Hence α is an irreducible in $Z[i]$.

(ii) Let us assume $2+3i = (a+bi)(c+di)$; $a,b,c,d \in Z$.

$\Rightarrow ac-bd = 2$, $ad+bc = 3$.

$\Rightarrow (a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2 = 2^2+3^2$

$= 13$.

either $a^2+b^2 = 1$, $c^2+d^2 = 13$ ~~$\Rightarrow (a+ib)(a-ib) = 1 \Rightarrow a+ib$~~

or $a^2+b^2 = 13$, $c^2+d^2 = 1$

$a^2+b^2 = 1 \Rightarrow (a+ib)\cdot(a-ib) = 1 \Rightarrow a+ib$ is a unit,

$c^2+d^2 = 1 \Rightarrow (c+id)\cdot(c-id) = 1 \Rightarrow c+id$ " " "

$\therefore$ In $2+3i = (a+bi)\cdot(c+di)$, either $(a+bi)$ is a unit or $(c+di)$ is a unit.

Hence $2+3i$ is an irreducible in $Z[i]$.

⑦ Find a gcd of the pair of elements in $\mathbb{Z}[i]$.

(iii) $2+3i,\ 4+5i$.

We define a norm function N on $\mathbb{Z}[i]$ by $N(a+bi) = a^2+b^2$.

Let $\alpha = a+bi$ is a common divisor of $2+3i$ and $4+5i$.

Then $N(\alpha) \mid N(2+3i)$ and $N(\alpha) \mid N(4+5i)$

i.e., $N(\alpha) \mid 13$ and $N(\alpha) \mid 41$

$\Rightarrow N(\alpha) = 1 \Rightarrow a^2+b^2 = 1 \Rightarrow a = \pm 1, b = 0;\ a = 0, b = \pm 1$.

These give 4 possible elements:

$1, -1, i, -i$ which are the units in $\mathbb{Z}[i]$

These are only one distinct element 1 with their associates. $\therefore$ 1 is a gcd of $2+3i$ and $4+5i$.

~~But i is not a divisor of $2+3i$, because~~

~~$(1+2i)(p+qi) = 2+3i$ gives~~

~~1 and is both are~~

(ii) $3-i,\ 4-3i$.

Let $\alpha = a+bi$ is a common divisor of $3-i$ & $4-3i$.

Then $N(\alpha) \mid N(3-i)$ and $N(\alpha) \mid N(4-3i)$

i.e., $N(\alpha) \mid 10$ and $N(\alpha) \mid 25$.

$\Rightarrow N(\alpha) = 1, 5$.

Let $\beta = c+di$ be a gcd. Then $N(\beta) = 5$

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

or $c = \pm 2,\ d = \pm 1$

These give 8 possible elements:

$1+2i, 1-2i, -1+2i, -1-2i$; $2+i, 2-i, -2+i, -2-i$. } These are two distinct elements $1+2i, 2+i$ with their associates

But $1+2i$ is not a divisor of $4-3i$, because

$(1+2i)(p+qi) = 4-3i$ gives $p-2q = 4,\ 2p+q = -3$.

$\Rightarrow p = \frac{4}{5}, q = -\frac{11}{5} \notin \mathbb{Z}$.

$\therefore$ $2+i$ is a gcd of $3-i$ and $4-3i$.

Exercise - 23 / S. K. Mapa / pg - 274.

(2) Prove that in a PID D, an element p is a prime if and only if p is irreducible.

Let p be a prime in a PID D. Therefore, $p \neq 0$, p is not a unit, ~~and $p|ab \Rightarrow$ either $p|a$ or $p|b$, for $a, b \in D$~~.

Let $a \in D$ and $a|p$. Then $p = ab$ for some $b \in D$.

$p = ab \Rightarrow p|ab$ and since p is a 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 $\exists$ some $d \in D$ s.t. $b = p \cdot d$

$\therefore p = a \cdot b = a \cdot pd$

$\Rightarrow p(1 - ad) = 0 \Rightarrow 1 - ad = 0$, since $p \neq 0$ and D is an I.D, contains no divisor of 0.

$\Rightarrow ad = 1$

$\Rightarrow a$ is a unit in D.

$\therefore a$ is a divisor of $p \Rightarrow$ either a is an associate of p or a is a unit in D.

$\therefore p$ is an irreducible in D.

Conversely,

Let p be irreducible in a PID D, and suppose that $p|ab$.

Then $\langle ab \rangle \subset \langle p \rangle$

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 $a|p$, which implies either a is a unit or $a \& p$ are associates.

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

Thus $\langle p \rangle$ 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.

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

$\Rightarrow$ either $p|a$ or $p|b$

$\Rightarrow p$ is a prime in D.

④ Express the ideal in the I.D. $\mathbb{Z}$ as a principal idea
(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, the ideal $3\mathbb{Z}+5\mathbb{Z}$ is a principal ideal
Let $p\mathbb{Z} = 3\mathbb{Z}+5\mathbb{Z}$. Then $3\mathbb{Z} \subset p\mathbb{Z}$, $5\mathbb{Z} \subset p\mathbb{Z}$.
$3\mathbb{Z} \subset p\mathbb{Z} \Rightarrow p|3$; $5\mathbb{Z} \subset p\mathbb{Z} \Rightarrow p|5$.
So p is a common divisor of 3 and 5.
Let d be any other common divisor of 3 & 5.
Then $d|3$ and $d|5$.
$\Rightarrow 3\mathbb{Z} \subset d\mathbb{Z}$ and $5\mathbb{Z} \subset d\mathbb{Z}$
$\Rightarrow 3\mathbb{Z}+5\mathbb{Z} \subset d\mathbb{Z} \Rightarrow p\mathbb{Z} \subset d\mathbb{Z} \Rightarrow d|p$.
i.e., p is the gcd of 3&5; i.e., $p = \gcd(3,5) = 1$.
Hence $3\mathbb{Z}+5\mathbb{Z} = \mathbb{Z}$.

(ii) Proceed in the similar way of (i),
p is the gcd of 8 & 12, i.e., $p = \gcd(8,12) = 4$
$\therefore$ $8\mathbb{Z}+12\mathbb{Z} = 4\mathbb{Z}$.

(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 $5|p$
So, p is a common multiple of 3 and 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 $m\mathbb{Z} \subset 5\mathbb{Z}$
$\Rightarrow m\mathbb{Z} \subset 3\mathbb{Z}\cap 5\mathbb{Z} \Rightarrow m\mathbb{Z} \subset p\mathbb{Z} \Rightarrow p|m$,
Thus p is the l.c.m. of 3 & 5
i.e., $p = 15$.
Hence $3\mathbb{Z}\cap 5\mathbb{Z} = 15\mathbb{Z}$.

⑤ If d be a gcd of three elements a, b, c in a PID D, show that d can be expressed as $d = au + bv + cw$ for some u, v, w in D.

Let us consider the principal ideals $\langle a\rangle, \langle b\rangle$ and $\langle c\rangle$ in D.

$\langle a\rangle + \langle b\rangle + \langle c\rangle$ is also an ideal in D.

Since D is a PID, $\langle a\rangle + \langle b\rangle + \langle c\rangle = \langle d\rangle$ for some $d \in D$.

$\Rightarrow \langle a\rangle \subset \langle d\rangle, \langle b\rangle \subset \langle d\rangle, \langle c\rangle \subset \langle d\rangle$.

$\Rightarrow d|a$, $d|b$ and $d|c$

$\Rightarrow d$ is a common divisor of a, b, c.

Let q be another common divisor of a, b, c.

$\therefore q|a$, $q|b$ and $q|c$

$\Rightarrow \langle a\rangle \subset \langle q\rangle, \langle b\rangle \subset \langle q\rangle, \langle c\rangle \subset \langle q\rangle$

$\Rightarrow \langle a\rangle + \langle b\rangle + \langle c\rangle \subset \langle q\rangle$; Since $\langle a\rangle + \langle b\rangle + \langle c\rangle$ is the smallest ideal containing $\langle a\rangle, \langle b\rangle$ and $\langle c\rangle$.

i.e., $\langle d\rangle \subset \langle c\rangle \Rightarrow c|d$

$\therefore d$ is a gcd of a, b and c.

Now $\langle d\rangle = \langle a\rangle + \langle b\rangle + \langle c\rangle \Rightarrow d|a$, $d|b$ and $d|c$

$\Rightarrow d = au + bv + cw$ for some $u, v, w \in D$.

⑥ Let D be a Euclidean domain with Euclidean valuation v. If b is a unit in D, prove that $v(ab) = v(a)$ for all non-zero $a \in D$

By the property of v in the Euclidean domain D, we have $v(a) \leq v(ab)$ for all non-zero $a, b \in D$.

Since b is a unit, $b \neq 0$, and $b^{-1} \in D$ s.t. $bb^{-1} = 1$.

Hence $v(a) = v(abb^{-1}) = v((ab)b^{-1}) \geq v(ab)$

$\therefore v(a) \leq v(ab)$ & $v(ab) \geq v(a)$

$\Rightarrow v(ab) = v(a)$ $\forall$ $a (\neq 0) \in D$.

⑧ Let D be a Euclidean domain with v. Prove that $v(1) < v(a)$ for all non-zero non-units $a \in D$.

Let $a \in D$ be a non-zero & non-unit element.

$\therefore 1a \neq 0$ in D, as D contains no divisor of zero.

By Euclidean domain property, $\exists$ elements q & r in D s.t. $1 = (1a)q + r$, either $r = 0$ or $v(r) < v(1a)$.

$r = 0 \Rightarrow 1 - (1a)q = 0 \Rightarrow 1(1 - aq) = 0 \Rightarrow 1 - aq = 0$ in D, $(1 \neq 0)$

$\Rightarrow a$ is a unit, a contradiction.

Therefore, $r = 0$ does not hold.
So $v(r) < v(1a)$.
But $v(r) = v[1(1-aq)] \geq v(1)$
$\therefore \quad v(1) < v(1a)$.
$\Rightarrow \quad \underline{v(1) < v(a)}$, $\forall$ non-zero non-units $a \in D$.

---

(11) (iii) Use Euclidean algorithm to find a gcd of the elements $a = 7+4i$, $b = 4+3i$ in $\mathbb{Z}[i]$ with a Euclidean valuation v defined by $v(m+ni) = m^2+n^2$. If d be a gcd, express d as $d = au+bv$ for some $u, v \in \mathbb{Z}[i]$.

$$\frac{7+4i}{4+3i} = \frac{(7+4i)(4-3i)}{(4+3i)(4-3i)} = \frac{40-5i}{25} = \frac{8-i}{5}$$
$$= (2+0i) - \left(\frac{2}{5} + \frac{1}{5}i\right)$$

a, $7+4i = 2(4+3i) - (4+3i)\left(\frac{2}{5}+\frac{1}{5}i\right)$
$= 2(4+3i) - (1+2i) = q(4+3i) + r$;
where $q = 2 \in \mathbb{Z}[i]$, $r = -1-2i \in \mathbb{Z}[i]$
and $v(r) = 5 < v(4+3i)$

Now $\frac{4+3i}{-1-2i} = \frac{(4+3i)(-1+2i)}{5} = \frac{-10+5i}{5} = -2+i$.

a, $4+3i = (-1-2i)(-2+i) = q_1(-1-2i) + r_1$;
where $q_1 = -2+i \in \mathbb{Z}[i]$, $r_1 = 0$.
The process terminates and $\underline{-1-2i \text{ is a gcd.}}$
We have, $7+4i = (4+3i)\cdot 2 + (-1-2i)$
a, $-1-2i = (7+4i)\cdot 1 + (4+3i)\cdot(-2)$.
$d = -1-2i = au+bv$, where $u = 1$, $v = -2 \in \mathbb{Z}[i]$.