STUDY MATERIALS

(RING THEORY-II)

TOPIC: UNIQUE FACTORIZATION DOMAIN

Mathematics Honours
Semester – 6

Paper – C14T Unit - 1

Dr. Sangita Chakraborty
Associate Professor
Department of Mathematics
Kharagpur College

UNIQUE FACTORIZATION DOMAIN.

UFD

- The Fundamental Theorem of Arithmetic can be extended from positive integers to the integers.
- The question arises of whether or not such factorizations are possibles in other rings.
- Generalizing this definition, we say:

An I.D. D is said to be a UFD, if D satisfies—

(i) Every non-zero and non-unit element $a \in D$ can be written as a product of irreducibles of D;

(ii) The factorization into irreducibles is unique upto associates and the order in which the factors appear. i.e., if $a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$; where p_i's, q_i's are irreducibles, then $r = s$ and p_i, q_j are associates for some i, j.

Examples:-

1. The I.D. $\mathbb{Z}$ is a UFD, by the Fundamental Theorem of Arithmetic.

   Because, every non-zero element of $\mathbb{Z}$ other than 1 and -1 (only units in $\mathbb{Z}$) can be expressed as the product of a finite number of irreducible elements in $\mathbb{Z}$ and the factorization is unique except for the orders and the associates of the irreducibles.

   eg. $18 = 2 \cdot 3 \cdot 3 = (-2) \cdot (-3) \cdot 3$; 3, -3 are associates.

Important Theorem:-

If D be a UFD then the polynomial ring D[x] is also a UFD.

So, $\mathbb{Z}[x]$ is a UFD, since $\mathbb{Z}$ is a UFD.

Theorem: In a UFD, every irreducible element is a prime.

Proof: Let p be an irreducible element in a UFD D.
Then $p \neq 0$ and p is not a unit in D.
Let $p \mid ab$; $a, b \in D$. Then $\exists\, k \in D$ s.t. $ab = pk$.
Since p is irreducible, and $p \mid ab$, at least one of a and b must be non-unit, as p being a non-unit.

Case 1. Let one of a and b be non-unit.
Let a be a unit, then $a^{-1} \in D$ and $b = a^{-1}(pk)$
$= p(ka^{-1})$.
$\therefore p \mid b$.
If b be a unit, then $b^{-1} \in D$ and $a = (pk)b^{-1} = p(kb^{-1})$
$\therefore p \mid a$
$\therefore p \mid a$ or $p \mid b$

Case 2. Let both of a and b be non-units.
Let $a = p_1 p_2 \cdots p_r$ and $b = q_1 q_2 \cdots q_s$ where $p_1, p_2, \cdots, p_r$; $q_1, q_2, \cdots, q_s$ are irreducibles in D.
If k be a unit, then $ab = pk \Rightarrow (ab)k^{-1} = p \Rightarrow ab \mid p$, again we have $p \mid ab \Rightarrow ab$ is an associate of p.
$\therefore ab$ is an irreducible, but it is not true.
$\therefore k$ is a non unit.
Let $k = t_1 t_2 \cdots t_K$; t_i's are irreducibles in D.
$ab = pk$ gives, $p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s = p t_1 t_2 \cdots t_K$.
By uniqueness of the factorisation of ab into irreducibles, it follows that —
p must be an associate of one of $p_1, p_2, \cdots, p_r$ or one of $q_1, q_2, \cdots, q_s$.
$\therefore p \mid a$ or $p \mid b$.
$\therefore p$ is a prime element in D.

Note: In a UFD there is no distinction between a prime element and an irreducible element.

Note: If an irreducible element in an I.D. be not a prime element, D is not a UFD.

Divisibility or Factorization in I.D.

If F be a field, then irreducible polynomials in F[x] may be considered as the building blocks in Polynomial ring; that is very similar to the building blocks (prime numbers) of the integers.

- Given an arbitrary I.D., we are led to the following series of definitions —

(i) Let D be an I.D. and $a, b \in D$ with $a \neq 0$. We say that a divides b (a/b) if there exists an element $c \in D$ s.t. $b = a.c$

(ii) A non-zero element a in an I.D. D is said to be a UNIT in D if a/I, I being the unity in D.
i.e., $\exists\ b \in D$ s.t. $a.b = I = b.a$
$\Rightarrow$ a has a multiplicative inverse in D.

(iii) Two non-zero elements a, b in an I.D. D are said to be Associates in D if there exists a unit u in D s.t. $a = b.u$.
$a = b.u \Rightarrow a.u^{-1} = b(u.u^{-1}) \Rightarrow a.u^{-1} = b.I = b$
$\Rightarrow b = a.v$, where $v = u^{-1}$, is also a unit in D.
$\therefore a = b.u \Rightarrow b = a.v$, where u, v are units in D.
Now a, b are associates in D $\Leftrightarrow a/b$ and b/a.
Because, a, b are associates in D $\Rightarrow a = b.u$, for some unit $u \in D$. $\Rightarrow b/a$
Also $a = b.u \Rightarrow b = a.u^{-1} \Rightarrow a/b$. } (proved)
conversely, a/b and $b/a \Rightarrow b = a.c$, $a = b.d$ for some $c, d \in D$.
$\therefore b = a.c = (b.d).c = b.(d.c)$
$\Rightarrow b.(I - d.c) = 0$, where $b \neq 0$.
$\Rightarrow I - d.c = 0$ in the I.D. D [D contains no divisor of zero]
$\Rightarrow d.c = I = c.d$ [$\because$ D is a commutative ring]
$\Rightarrow$ Both c and d are units in D. $\Rightarrow$ a, b are associates.

NOTE:- Units in an I.D. D and the associates of a non-zero $a \in D$ are always called improper divisors of a.

Because, $a = a.I = a.(uu^{-1})$ for some unit $u \in D$.

$\Rightarrow a = (au).u^{-1} \Rightarrow au \mid a$ and $u^{-1} \mid a$.

All other divisors (if any) except units and associates of a are called proper divisors of a.

For example, in the I.D. $\mathbb{Z}$, the improper divisors of 12 are 1, -1, 12 and -12. The proper divisors of 12 are 2, -2, 3, -3, 4, -4, 6, -6.

(iv) Multiplicative Norm Function on an I.D.

Definition → A norm function N on an I.D. D is a mapping $N : D \longrightarrow \mathbb{Z}$ satisfies the following—

(1) $N(\alpha) \geq 0$, $\forall \alpha \in D$.

(2) $N(\alpha) = 0$ iff $\alpha = 0$ in D.

(3) $N(\alpha.\beta) = N(\alpha).N(\beta)$, $\forall \alpha, \beta \in D$.

NOTE: $N(u) = 1$ for every unit $u \in D$.

For, $N(I.I) = N(I).N(I)$, by (3)

$\Rightarrow N(I) = N(I).N(I) \Rightarrow N(I)(1 - N(I)) = 0$ in $\mathbb{Z}$

$\Rightarrow 1 - N(I) = 0$, since $N(I) \neq 0$ and $\mathbb{Z}$ is an I.D., containing no divisors of zero.

$\Rightarrow N(I) = 1$ in $\mathbb{Z}$.

If u be a unit in D, then $u^{-1} \in D$ and $uu^{-1} = I$

$\therefore N(uu^{-1}) = N(I) \Rightarrow N(u).N(u^{-1}) = 1$, by (3).

$\Rightarrow N(u) = 1$, $\forall$ unit u in D.

(v) Greatest Common Divisor (gcd) :-

Let D be an I.D. and $a, b \in D$ s.t. $a \neq 0, b \neq 0$.

An element $d \in D$ is said to be a gcd of a and b if

1. $d \mid a$ and $d \mid b$
2. $c \mid a$ and $c \mid b \Rightarrow c \mid d$ for any $c \in D$.

NOTE: If d be a gcd of a and b, then d.u is also a gcd, u being a unit.

1. Any two gcd's of two elements, if they exist, are associates.

For, Let c, d be two gcd's of a and b in D.
Since $c|a$, $c|b$ and d is a gcd, $c|d$ $\Rightarrow$ c, d are
Again, since $d|a$, $d|b$ and c " " " , $d|c$ associates in D.

Note: In a I.D., two elements may not have a gcd.

2. Two non-zero elements a and b in an I.D. D are said to be prime to each other if gcd of a and b is a unit.

(vi) Least Common Multiple (lcm) :-
Let D be an I.D. and $a(\neq 0)$, $b(\neq 0)$ be in D
An element $l \in D$ is said to be a lcm of a and b if
1. $a|l$ and $b|l$
2. $a|m$ and $b|m \Rightarrow l|m$ for any $m \in D$.

Note: Any two lcm's of a and b in an I.D. are associates.

(vii) Irreducible element :-
A non-zero element a in an I.D. D is said to be an irreducible element in D if
1. a is not a unit in D,
2. the only divisors of a are units in D and the associates of a.

Equivalently,
A non-zero element a in an I.D. D that is not a unit in D is said to be irreducible whenever $a = b.c$, either b is a unit in D and c is an associate of a or reversely.

Note: 1. An associate of an irreducible element in D is also an irreducible in D.
2. There is no irreducible element in a field.
For, a field is a I.D. and every non-zero element in a field is a unit.

(viii) **Prime Element :-** A non-zero element p in an I.D. D is said to be a prime element in D if
1. p is not a unit,
2. $p \mid ab \Rightarrow$ either $p \mid a$ or $p \mid b$ for $a, b \in D$.

Theorem: In an I.D., every prime element is an irreducible.

Converse is NOT TRUE in general.

Proof :- Let p be a prime element in an I.D. D.
Then $p \neq 0$ and p is not a unit in D.
Let $a \in D$ s.t. $a \mid p$. Then $\exists$ some $b \in D$ s.t.
$p = a \cdot b \Rightarrow p \mid a \cdot b \Rightarrow$ either $p \mid a$ or $p \mid b$ [$\because p$ is a prime]

Case 1. If $p \mid a$, then we have $p \mid a$ and $a \mid p$
$\Rightarrow a$ is an associate of p.

Case 2. If $p \mid b$, then $\exists$ some $c \in D$ s.t. $b = p \cdot c$.
$\therefore p = a \cdot b = a \cdot (p \cdot c) = p \cdot (a \cdot c)$
$\Rightarrow p \cdot (1 - a \cdot c) = 0 \Rightarrow 1 - a \cdot c = 0$ [$\because p \neq 0$ and D is an I.D.]
$\Rightarrow a \cdot c = 1 \Rightarrow a$ is a unit in D.

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

Converse is : An irreducible element may not be a prime in an I.D.

Example: In the I.D. $D = \mathbb{Z}[\sqrt{-3}]$, $4 = 2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$.
2 is an irreducible element in D. Because, if $2 = (a+b\sqrt{-3})(c+d\sqrt{-3})$, and we define a norm function N on D by $N(a+b\sqrt{-3}) = a^2+3b^2$,
then $N(2) = N(a+b\sqrt{-3}) \cdot N(c+d\sqrt{-3}) = (a^2+3b^2)(c^2+3d^2)$
$\Rightarrow 2^2 = (a^2+3b^2) \cdot (c^2+3d^2)$; where $a, b, c, d \in \mathbb{Z}$.
$\therefore$ either (i) $a^2+3b^2 = 1$; $c^2+3d^2 = 4 \rightarrow \{a = \pm 1, b = 0$; $c = \pm 1, d = \pm 1$; $c = \pm 2, d = 0\}$
or (ii) $a^2+3b^2 = 4$; $c^2+3d^2 = 1 \rightarrow \{a = \pm 1, b = \pm 1$; $a = \pm 2, b = 0$; $c = \pm 1, d = 0\}$
or (iii) $a^2+3b^2 = 2$; $c^2+3d^2 = 2 \rightarrow$ cannot hold.
From (i) & (ii) $\Rightarrow$ either $a+b\sqrt{-3}$ (± 1) or $c+d\sqrt{-3}$ (± 1) is a unit
$\therefore$ 2 is irreducible.

Now $2.2 = (1+\sqrt{-3})\cdot(1-\sqrt{-3}) \Rightarrow 2 \mid (1+\sqrt{-3})(1-\sqrt{-3})$.
But $2 \nmid (1+\sqrt{-3})$ and $2 \nmid (1-\sqrt{-3})$.
For, if $2 \mid (1+\sqrt{-3})$, then $1+\sqrt{-3} = 2\cdot K$, $K \in \mathbb{Z}[\sqrt{-3}]$
or, $(\sqrt{-3})^2 = (2K-1)^2 \Rightarrow K^2 - K + 1 = 0$
$\Rightarrow K = \frac{1}{2} \pm \frac{1}{2}\sqrt{-3} \notin \mathbb{Z}[\sqrt{-3}]$.

$\therefore$ 2 is neither a divisor of $1+\sqrt{-3}$ nor a divisor of $1-\sqrt{-3}$.
$\therefore$ 2 is not a prime though it is an irreducible in $\mathbb{Z}[\sqrt{-3}]$.

Ex. Find the units in the I.D. $\mathbb{Z}[x]$.
The identity (unity) element in the I.D. $\mathbb{Z}[x]$ is the constant polynomial 1.
Let $f(x) \in \mathbb{Z}[x]$ be a unit.
Then $f(x) \neq 0$ and $\exists$ some $g(x) \neq 0$ in $\mathbb{Z}[x]$ s.t. $f(x)\cdot g(x) = 1$.
$\Rightarrow \deg(f(x)\cdot g(x)) = \deg(1) = 0$
$\Rightarrow \deg(f(x)) + \deg(g(x)) = 0$ [$\because \mathbb{Z}[x]$ is an I.D.]
$\Rightarrow \deg(f(x)) = 0 = \deg(g(x))$
$\Rightarrow$ Both $f(x)$ and $g(x)$ are non-zero constant polynomials in $\mathbb{Z}[x]$.
$\therefore$ The units in $\mathbb{Z}[x]$ are also the units in the I.D. $\mathbb{Z}$.
Hence the units are 1 and -1.

Ex. 1.(ii). Find the units in the I.D. $\mathbb{Z}[\sqrt{-3}]$.
Let us define a norm function on $\mathbb{Z}[\sqrt{-3}]$ as $N(\alpha) = \alpha\cdot\bar{\alpha} = a^2 + 3b^2$; where $\alpha = a + b\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$.
$\therefore N(\alpha) \geq 0 \ \forall \alpha \in \mathbb{Z}[\sqrt{-3}]$ and $N(\alpha) = 0$ iff $\alpha = 0$.
$N(\alpha.\beta) = N(\alpha)\cdot N(\beta)$ for taking $\beta = c + d\sqrt{-3}$,
then $N(\alpha.\beta) = N\{(a+b\sqrt{-3})\cdot(c+d\sqrt{-3})\} = N\{(ac-3bd)+(bc+ad)\sqrt{-3}\}$
$= (ac-3bd)^2 + 3(bc+ad)^2 = a^2c^2 + 9b^2d^2 + 3b^2c^2 + 3a^2d^2 - 6abcd + 6abcd = (a^2+3b^2)(c^2+3d^2)$
And $N(\alpha)\cdot N(\beta) = (a^2+3b^2)\cdot(c^2+3d^2)$
$\therefore N(\alpha.\beta) = N(\alpha)\cdot N(\beta)$, $\forall \alpha, \beta \in \mathbb{Z}[\sqrt{-3}]$.

$\therefore$ N is a norm function on $\mathbb{Z}[\sqrt{-3}]$.

Let $\alpha = a+b\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$ is a unit.

Then $N(\alpha)=1 \Rightarrow \alpha\cdot\bar{\alpha}=1 \Rightarrow a^2+3b^2=1$; $a,b\in\mathbb{Z}$

$\Rightarrow a=\pm1,\ b=0$.

$\therefore \alpha = a+b\sqrt{-3} = \pm 1$.

Hence the units in $\mathbb{Z}[\sqrt{-3}]$ are 1 and -1.

[which are also only units in $\mathbb{Z}$].

6. For an element $\alpha = a+bi$ in the domain $\mathbb{Z}[i]$, a^2+b^2 is a prime integer.
Prove that α is an irreducible element in $\mathbb{Z}[i]$.
Show that $2+3i$ is " " " $\mathbb{Z}[i]$.

1st part. We define a norm function N on the domain $\mathbb{Z}[i]$ by $N(\alpha)=N(a+bi)=\alpha\cdot\bar{\alpha}=a^2+b^2=p$ (prime), say.

Let $\alpha=\beta\gamma \Rightarrow N(\alpha)=N(\beta)\cdot N(\gamma)$; $\alpha,\beta,\gamma\in\mathbb{Z}[i]$.

$\therefore p=N(\beta)\cdot N(\gamma) \Rightarrow$ either $N(\beta)=1$ or $N(\gamma)=1$.

$\therefore$ either β is a unit or γ is a unit.

$\therefore$ α is an irreducible in $\mathbb{Z}[i]$.

2nd Part.

Let we assume $2+3i=(a+bi)\cdot(c+di)$; $a,b,c,d\in\mathbb{Z}$.

$\Rightarrow (ac-bd)+i(ad+bc)=2+3i$

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

Now $(a^2+b^2)\cdot(c^2+d^2)=(ac-bd)^2+(ad+bc)^2=2^2+3^2=13$.

either (i) $a^2+b^2=1,\ c^2+d^2=13$

or (ii) $a^2+b^2=13,\ c^2+d^2=1$.

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

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

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

$\Rightarrow$ $2+3i$ is an irreducible element in $\mathbb{Z}[i]$.

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

On the domain $\mathbb{Z}[\sqrt{-5}] = \{a+b\sqrt{-5} : a, b \in \mathbb{Z}\}$,

$21 = 3.7 = (1+2\sqrt{-5})\cdot(1-2\sqrt{-5})$.

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

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

Let us define a Norm function N on $\mathbb{Z}[\sqrt{-5}]$ as:

$N(a+b\sqrt{-5}) = a^2+5b^2$.

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

$\Rightarrow 3^2 = (a^2+5b^2)\cdot(c^2+5d^2)$.

$\Rightarrow$ either (i) $a^2+5b^2=1$ and $c^2+5d^2=9$, $\Rightarrow$ $a=\pm1, b=0$; $c=\pm3, d=0$, $c=\pm2, d=\pm1$

or (ii) $a^2+5b^2=9$ and $c^2+5d^2=1$, $\Rightarrow$ $a=\pm3, b=0$, $a=\pm2, b=\pm1$; $c=\pm1, d=0$

or (iii) $a^2+5b^2=3$ and $c^2+5d^2=3$ $\Rightarrow$ can not happen.

So in (i) $a+b\sqrt{-5}$ is a unit and in (ii) $c+d\sqrt{-5}$ is a unit.

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

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

Similarly, 7 is " " "

To Show: $1+2\sqrt{-5}$ is irreducible in $\mathbb{Z}[\sqrt{-5}]$.

Let $1+2\sqrt{-5} = (p+q\sqrt{-5})\cdot(r+s\sqrt{-5})$; $p,q,r,s \in \mathbb{Z}$.

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

$\Rightarrow 1^2+5\cdot2^2 = 21 = (p^2+5q^2)\cdot(r^2+5s^2)$

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

or (iii) $p^2+5q^2=3$, $r^2+5s^2=7$.

or (iv) $p^2+5q^2=7$, $r^2+5s^2=3$, } Do not happen.

So in (i) $p+q\sqrt{-5}$ $(=\pm1)$ is a unit and

in (ii) $r+s\sqrt{-5}$ (±1) " " " in $\mathbb{Z}[\sqrt{-5}]$.

$\therefore$ $1+2\sqrt{-5}$ is irreducible in $\mathbb{Z}[\sqrt{-5}]$.

Similarly, $1-2\sqrt{-5}$ is also an irreducible in $\mathbb{Z}[\sqrt{-5}]$.
∴ We have two different factorizations of $21 = 3\cdot 7 = (1+2\sqrt{-5})\cdot(1-2\sqrt{-5})$ 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 $\mathbb{Z}[\sqrt{-5}]$. [as $1\pm 2\sqrt{-5} \neq (\pm 1)3$ or $(\pm 1)7$]
∴ The domain $\mathbb{Z}[\sqrt{-5}]$ is NOT a UFD.

(4) Show that 2 is an irreducible in the domain $D = \mathbb{Z}[\sqrt{-6}]$. Using $2\cdot 5 = (2+\sqrt{-6})\cdot(2-\sqrt{-6})$, 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 $2 = (a+b\sqrt{-6})\cdot(c+d\sqrt{-6})$; $a, b, c, d \in \mathbb{Z}$.
∴ $N(2) = N(a+b\sqrt{-6})\cdot N(c+d\sqrt{-6})$
$\Rightarrow 4 = (a^2+6b^2)\cdot(c^2+6d^2)$.
$\Rightarrow$ either (i) $a^2+6b^2=1$, $c^2+6d^2=4$; $\Rightarrow a=\pm 1, b=0$; $c=\pm 2, d=0$.
or (ii) $a^2+6b^2=4$, $c^2+6d^2=1$; $\Rightarrow a=\pm 2, b=0$; $c=\pm 1, d=0$.
or (iii) $a^2+6b^2=2$, $c^2+6d^2=2$; $\Rightarrow$ This cannot happen.
In (i) $a+b\sqrt{-6}$ $(=\pm 1)$ is a unit, and in (ii) $c+d\sqrt{-6}$ $(=\pm 1)$ is a unit in D.
∴ if $2 = (a+b\sqrt{-6})\cdot(c+d\sqrt{-6})$, then either $a+b\sqrt{-6}$ or $(c+d\sqrt{-6})$ is a unit.
∴ 2 is irreducible in D.

From $2\cdot 5 = (2+\sqrt{-6})\cdot(2-\sqrt{-6})$, we get
$2 \mid (2+\sqrt{-6})\cdot(2-\sqrt{-6})$.
But $2 \nmid (2+\sqrt{-6})$ and $2 \nmid (2-\sqrt{-6})$. For, if $2 \mid (2\pm\sqrt{-6})$ then $2\cdot(p+q\sqrt{-6}) = 2\pm\sqrt{-6} \Rightarrow 2p=2$, $2q=\pm 1$
$\Rightarrow p=1 \in \mathbb{Z}$, but $q = \pm\frac{1}{2} \notin \mathbb{Z}$.
Hence 2 is a prime in D.

To show: D is not a UFD.
We have shown that 2 is irreducible in D.
Similarly we can show that 5, $2\pm\sqrt{-6}$ are also irreducible in D.

Now from $10 = 2\cdot 5 = (2+\sqrt{-6})\cdot(2-\sqrt{-6})$, we have two different factorizations 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 only units in D. [$\because 2\pm\sqrt{-6} \neq (\pm 1)\cdot 2$; $2\pm\sqrt{-6} \neq (\pm 1)\cdot 5$]
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 $\alpha = 21 = 3\cdot 7 = (1+2\sqrt{-5})\cdot(1-2\sqrt{-5})$, $\beta = 3(1+2\sqrt{-5})$
Let us define a norm function N on $D = \mathbb{Z}[\sqrt{-5}]$ by $N(a+b\sqrt{-5}) = a^2+5b^2$; $a, b \in \mathbb{Z}$.
3 is a common divisor of α and β.
$(1+2\sqrt{-5})$ " " " " " " " "
Let $\gamma = 3$ and $\delta = 1+2\sqrt{-5}$; and $d = p+q\sqrt{-5}$ be a gcd of α and β; $p, q \in \mathbb{Z}$.
Then $N(d) \mid N(\alpha)$ and $N(d) \mid N(\beta)$
i.e., $N(d) \mid N(21)$ and $N(d) \mid N\{3(1+2\sqrt{-5})\}$
$\Rightarrow$ $N(d) \mid 441$ and $N(d) \mid 9\cdot 21$
$\therefore$ Possible values of $N(d)$: 1, 3, 7, 9, 21, 63.
Since $d = \gcd(\alpha, \beta)$ and γ, δ are common divisors of α, β, then $N(\gamma) \mid N(d)$ and $N(\delta) \mid N(d)$.
Now $N(\gamma) = 9$, $N(\delta) = 21$.
$\therefore$ $N(d) = 63 \Rightarrow p^2+5q^2 = 63$
$\exists$ no integers p and q s.t. $p^2+5q^2 = 63$.
$\therefore$ There is no element in D which can be a gcd of α and β.

2ND Part: Since any two elements 21 and $3(1+2\sqrt{-5})$ in D have no gcd, it follows that D is NOT a UFD, since in a UFD, any two non-zero elements have a gcd.

7. Find a gcd of the pair of elements in $\mathbb{Z}[i]$.
(i) $2+3i$, $4+5i$; (ii) $3-i$, $4-3i$.

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

Let $\alpha = a+bi \in \mathbb{Z}[i]$, be a common divisor of $2+3i$ and $4+5i$.

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

i.e, $N(\alpha) \mid (2^2+3^2)$ and $N(\alpha) \mid (4^2+5^2)$

or, $N(\alpha) \mid 13$, $N(\alpha) \mid 41$

$\Rightarrow$ $N(\alpha) = 1$ [$\because$ gcd(13, 41) = 1]

$\Rightarrow$ $a^2+b^2 = 1 \Rightarrow a = \pm 1, b = 0$; $a = 0, b = \pm 1$.

We get $\alpha = 1, -1, i, -i$; which are the units in $\mathbb{Z}[i]$. ~~So these are the 4 common divisors. Here 1 and i are only two distinct elements with their associates.~~

~~$\therefore$ 1 is a gcd of $2+3i$ and $4+5i$.~~

So $1, -1, i, -i$ are 4 common divisors ; and there is only one distinct element 1 with its associates -1, i and $-i$.

$\therefore$ 1 is a gcd of $2+3i$ and $4+5i$

(ii) Let $\alpha = a+bi$ is a common divisor of $3-i$ and $4-3i$.

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

$\Rightarrow$ $N(\alpha) \mid (3^2+1^2)$; $\Rightarrow N(\alpha) \mid (4^2+3^2)$

$\Rightarrow$ $N(\alpha) \mid 10$; $\Rightarrow N(\alpha) \mid 25$.

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

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 ;–

$1+2i$, $1-2i$, $-1+2i$, $-1-2i$; $2+i$, $2-i$, $-2+i$, $-2-i$.

There exist two distinct elements $1+2i$ and $2+i$ with their associates.

But $(1+2i) \nmid (4-3i)$, since if

$(1+2i)(p+qi) = 4-3i$, for $p+qi \in \mathbb{Z}[i]$,

then $p-2q = 4$, $2p+q = -3 \Rightarrow p = 42/5 \notin \mathbb{Z}$, $q = -11/5 \notin \mathbb{Z}$

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