(126)

Def: (Irreducible element)

A nonzero, nonunit element $\alpha \in \mathbb{Z}[\sqrt{d}]$ is an irreducible element if

$$\alpha = \beta\gamma$$

implies either β or γ is a unit, $\beta, \gamma \in \mathbb{Z}[\sqrt{d}]$.

Exc: 3 is an irreducible element in $\mathbb{Z}[\sqrt{-5}]$

Solution: On contrary, suppose

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

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

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

Case 1:

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

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

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

(127)

Case 2: $a^2+5b^2=9$ & $c^2+5d^2=1$

$c+d\sqrt{-5} = \pm 1$ is a unit.

Case 3: $a^2+5b^2=3$ &

$c^2+5d^2=3$

This is not possible.

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

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

As $3 \mid 9 \Rightarrow 3 \mid (2+\sqrt{-5})(2-\sqrt{-5})$

If $3 \mid 2+\sqrt{-5}$ then

$$2+\sqrt{-5} = 3(a+b\sqrt{-5})$$

$\Rightarrow 3a = 2 \Rightarrow a = \frac{2}{3}$. a contradiction

as $a \in \mathbb{Z}$

$\therefore 3 \nmid 2+\sqrt{-5}$, Similarly $3 \nmid 2-\sqrt{-5}$

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

Every Prime element is irreducible but converse is not true always.

<u>Proof:</u> consider $\beta \in \mathbb{Z}[\sqrt{-d}]$ be a prime element. To prove β is an irreducible element.

On contrary, assume

$$\beta = \gamma\delta \quad (*), \quad \gamma, \delta \in \mathbb{Z}[\sqrt{-d}]$$

neither γ, nor δ is a unit

Now $N(\beta) = N(\gamma)\, N(\gamma)$

Since β is a prime element

$\therefore\ \beta \mid \gamma$ or $\beta \mid \delta$

If $\beta \mid \gamma$, then $\gamma = \beta \cdot c$, $c \in \mathbb{Z}[\sqrt{-d}]$

From $(*)$ $1 = c\delta$

$\Rightarrow \delta$ is a unit

Similarly if $\beta \mid \delta$ then γ is a unit

(129)

A contradiction to our assumption.
Hence β is an irreducible element.

Converse is not true.

~~e.g 3 is an irreducible element but~~

e.g: 3 is not a prime element but ~~not~~ an irreducible element.

(130)

Unique Factorization Domain (U.F.D)

Def: An Integral domain R with unity is called a U.F.D if it satisfies the following conditions.

(i) Each nonzero element of R is either a unit or canbe expressed as a product of finite number of irreducible elements of R.

(ii) The above decomposition is unique upto order and associates of the irreducible of R.

1. Every field F is a U.F.D $\because$ every element of field is a unit.

2. $\mathbb{Z}$ is a U.F.D.

(131)

3. $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$, $F[x]$ are U.F.D.

4. $\mathbb{Z}[\sqrt{-3}]$, $\mathbb{Z}[\sqrt{-14}]$ are not U.F.D

~~Theorem~~ <u>Excercise</u>: Unique Factorization does not hold always in $\mathbb{Z}[\sqrt{d}]$.

e.g: 1. $\mathbb{Z}[\sqrt{-14}]$: Units : ± 1

$$15 = 3 \cdot 5$$

$$15 = (1+\sqrt{-14})(1-\sqrt{-14})$$

has two factorizations.

2. $K = \mathbb{Q}[\sqrt{-5}]$, $R = \mathbb{Z}[\sqrt{-5}]$

$$6 = 2 \cdot 3$$

$$= (1+\sqrt{-5})(1-\sqrt{-5})$$

has two factorization

$\Rightarrow$ Unique factorization does not hold.