<u>Proposition:</u> Let α be an element of $\mathbb{Z}[\sqrt{d}]$. If $N(\alpha)$ is prime in $\mathbb{Z}$ then α is prime in $\mathbb{Z}[\sqrt{d}]$.

<u>Proof:</u> Let $\alpha \in \mathbb{Z}[\sqrt{d}]$

and $\alpha = \beta\gamma$; $\beta, \gamma \in \mathbb{Z}[\sqrt{d}]$.

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

As $N(\alpha) \in \mathbb{Z}$ is prime

$\Rightarrow$ $N(\beta) = \pm 1$ or $N(\gamma) = \pm 1$

$\Rightarrow$ Either β is a Unit or γ is a Unit.

$\Rightarrow$ $\alpha \mid \gamma$ or $\alpha \mid \beta$

$\Rightarrow$ α is prime as it is not zero and not a unit as $N(\alpha)$ is prime.

123

<u>Converse is not true.</u>

e.g $\alpha = 3$

$N(\alpha) = 9$ is not a prime in $\mathbb{Z}$

but 3 is a prime in $\mathbb{Z}[i]$.

<u>Exc</u>: $2+i$ and $2-i$ are primes in $\mathbb{Z}[i]$ as

$N(2+i) = 5$ is prime in $\mathbb{Z}$

and

also $N(2-i) = 5$ is prime in $\mathbb{Z}$.

(124)

Proposition: Every non zero element of $\mathbb{Z}[\sqrt{d}]$ that is not a unit can be factored as a product of primes in $\mathbb{Z}[\sqrt{d}]$.

Proof: We will prove by induction on $|N(\alpha)|$. As units and 0 are excluded, therefore induction starts with $|N(\alpha)| = 2$.

As $N(\alpha) = 2$, a prime

$\Rightarrow$ α is a prime.

→ For induction step, all elements with

$$N(\beta) < N(\alpha), \forall \beta \in \mathbb{Z}[\sqrt{d}]$$

can be written as a product of primes in $\mathbb{Z}[\sqrt{d}]$.

→ If α is a prime, there is nothing to prove.

(125)

If α is not a prime, i.e,

$\alpha = \beta\gamma$

neither β nor γ is a unit.

$\therefore$ $N(\beta) > 1$ & $N(\gamma) > 1$

Since $N(\alpha) = N(\beta) N(\gamma)$

$\Rightarrow$ $|N(\beta)| < |N(\alpha)|$

& $|N(\gamma)| < |N(\alpha)|$

$\Rightarrow$ By Induction hypothesis, β and γ are product of primes in $\mathbb{Z}[\sqrt{d}]$, hence α is a product of prime.