(112)

Theorem: The integers of K are $\{a+b\sqrt{d} \mid a,b \in \mathbb{Z}\}$ if $d \not\equiv 1 \pmod 4$ and $\{a+b\left(\frac{1+\sqrt{d}}{2}\right) \mid a,b \in \mathbb{Z}\}$ if $d \equiv 1 \pmod 4$

Proof: Firstly we will prove both the sets consists of integers in K.

(i) If $\alpha = a+b\sqrt{d}$, $a,b \in \mathbb{Z}$

$$Tr(\alpha) = 2a \in \mathbb{Z}$$

$$N(\alpha) = a^2 - db^2 \in \mathbb{Z}$$

(ii) If $\alpha = a+b\left(\frac{1+\sqrt{d}}{2}\right)$, $a,b \in \mathbb{Z}$

$$= \left(a+\frac{b}{2}\right) + \frac{b}{2}\sqrt{d}$$

$$Tr(\alpha) = 2\left(a+\frac{b}{2}\right) = 2a+b \in \mathbb{Z}$$

(113)

$$N(\alpha) = \left(a + \frac{b}{2}\right)^2 - \frac{db^2}{4}$$

$$= a^2 + \frac{b^2}{4} + ab - \frac{db^2}{4}$$

$$= a^2 + ab + \frac{b^2}{4}(1-d)$$

$$= a^2 + ab + b^2\left(\frac{1-d}{4}\right)$$

As $d \equiv 1 \pmod 4$

$\therefore$ $N(\alpha) \in Z'$

$\Rightarrow \{ a + b\sqrt{d} \mid a, b \in Z' \}$ and

$\{ a + b\left(\frac{1+\sqrt{d}}{2}\right) \mid a, b \in Z' \}$

represents integers in K.

We have to show conversely that every integer of K has the indicated form.

(114)

Let $\alpha = x + y\sqrt{d}$ be an integer of K.

$\Rightarrow Tr(\alpha) = 2x \in \mathbb{Z}$

$N(\alpha) = x^2 - dy^2 \in \mathbb{Z}$

$\Rightarrow$ Either $x \in \mathbb{Z}$ or x is half an odd integer.

If $x \in \mathbb{Z}$ then $x^2 \in \mathbb{Z}$

$\Rightarrow dy^2 \in \mathbb{Z} \Rightarrow y \in \mathbb{Z}$

(∵ d is square free & if $y = \frac{a}{b}$

$y^2 = \frac{a^2}{b^2}$, $b^2 \mid d b^2 \Rightarrow y \in \mathbb{Z}$)

If x is half an odd integer.

$x = \frac{a}{2}$, $a \in \mathbb{Z}$ is an odd integer.

$N(\alpha) = x^2 - dy^2 = \frac{a^2}{4} - dy^2 \in \mathbb{Z}$

(115)

Now $a^2 - d(2y)^2 \in 4\mathbb{Z}$ — (*)

$\Rightarrow d(2y)^2 \in \mathbb{Z}$

$\Rightarrow 2y \in \mathbb{Z}$ $\because$ d is square free

Either $y \in \mathbb{Z}$ or y is half an odd integer.

If $y \in \mathbb{Z}$ then

$a^2 - 4dy^2$ is odd $\because$ a is odd

A contradiction to (*)

$\therefore$ $y = \frac{b}{2}$, b is odd integer

So $\alpha = x + y\sqrt{d} = \frac{a}{2} + \frac{b}{2}\sqrt{d}$

$= \frac{a-b}{2} + b\left(\frac{1+\sqrt{d}}{2}\right)$

as $2 \mid a-b \Rightarrow \alpha$ has the form as in the statement.

Remark: $K = \mathbb{Q}[\sqrt{d}]$

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \not\equiv 1 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{4}\right] & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

$\mathcal{O}_K$ is called the ring of integers and is a subring of K.

K	$\mathcal{O}_K$
$\mathbb{Q}[i]$	$\mathbb{Z}[i]$
$\mathbb{Q}[\sqrt{2}]$	$\mathbb{Z}[\sqrt{2}]$
$\mathbb{Q}[\sqrt{5}]$	$\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$
$\mathbb{Q}[\sqrt{-5}]$	$\mathbb{Z}[\sqrt{-5}]$
$\mathbb{Q}[\sqrt{-14}]$	$\mathbb{Z}[\sqrt{-14}]$

117

Theorem: Prove that the Trace is additive and the norm is multiplicative ie

$$Tr(\alpha+\beta) = Tr(\alpha) + Tr(\beta)$$

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

Proof: Let $\alpha, \beta \in K = \mathbb{Q}[\sqrt{d}]$

$$\alpha = a_1 + b_1\sqrt{d} \;;\; a_1, b_1 \in \mathbb{Q}$$

$$\beta = a_2 + b_2\sqrt{d} \;;\; a_2, b_2 \in \mathbb{Q}$$

$$\alpha+\beta = (a_1+a_2) + (b_1+b_2)\sqrt{d} \in K$$

$$Tr(\alpha+\beta) = 2(a_1+a_2)$$

$$= 2a_1 + 2a_2$$

$$= Tr(\alpha) + Tr(\beta)$$

$$N(\alpha+\beta) = (a_1+a_2)^2 - d(b_1+b_2)^2$$

$$\alpha\beta = (a_1a_2 + b_1b_2d) + \sqrt{d}(a_1b_2 + a_2b_1)$$

(118)

$$N(\alpha\beta) = (a_1 a_2 + b_1 b_2 d)^2 - d(a_1 b_2 + a_2 b_1)^2$$

$$= (a_1^2 - d b_1^2)(a_2^2 - d b_2^2)$$

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

Units: A nonzero element $\alpha \in \mathbb{Z}[\sqrt{a}]$ is called Unit if α^{-1} also lies in $\mathbb{Z}[\sqrt{a}]$.

e.g $\mathbb{Z}[i]$, Units are $\pm 1, \pm i$

Prime: An element $\alpha \in \mathbb{Z}[\sqrt{a}]$ is said to be prime in $\mathbb{Z}[\sqrt{a}]$ if it is neither zero nor a Unit and

$$\alpha \mid \beta\gamma \Rightarrow \text{either } \alpha \mid \beta \text{ or } \alpha \mid \gamma$$

Remark: An integer p in $\mathbb{Z}$ can be prime in $\mathbb{Z}$ but not prime in $\mathbb{Z}[\sqrt{a}]$

(20)

e.g $\mathbb{Z}[i]$, $d = -1$

$$5 = (2+i)(2-i)$$

5 is not a prime in $\mathbb{Z}[i]$

as $5 \nmid 2+i$ and $5 \nmid 2-i$

but 5 is not a prime in $\mathbb{Z}[i]$.

Proposition: An element $\alpha \in \mathbb{Z}[\sqrt{d}]$ is a unit iff $N(\alpha) = \pm 1$.

Proof: Suppose α is a unit in $\mathbb{Z}[\sqrt{d}]$.

$\Rightarrow \alpha^{-1} \in \mathbb{Z}[\sqrt{d}]$.

Now $N(\alpha)\, N(\alpha^{-1}) = N(\alpha\alpha^{-1})$

$= N(1) = 1$

$\Rightarrow N(\alpha) = \pm 1$

(12)

Conversely, Let $N(\alpha) = \pm 1$

$\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, $a, b \in \mathbb{Z}$

To prove α is a unit in $\mathbb{Z}[\sqrt{d}]$

i.e. $\alpha^{-1} = a + b\sqrt{d}$

$\alpha\alpha^{-1} = 1 \Rightarrow \alpha^{-1} = \frac{1}{\alpha}$

$= \frac{1}{a+b\sqrt{d}}$

$= \frac{a-b\sqrt{d}}{a^2 - db^2}$

$= \frac{a-b\sqrt{d}}{N(\alpha)}$

$= \pm 1(a - b\sqrt{d}) \in \mathbb{Z}[\sqrt{d}]$

$\Rightarrow \alpha^{-1} \in \mathbb{Z}[\sqrt{d}]$

$\Rightarrow \alpha$ is a unit in $\mathbb{Z}[\sqrt{d}]$.