Lecture 2

<u>Qus.</u> What is the integer ring of $\mathbb{Q}$

<u>Ans:</u> It is $\mathbb{Z}$. $\Leftarrow$ First prop of Lec 1.

<u>Theorem</u>: Let d be a square-free integer. Then the ring of integers of $\mathbb{Q}(\sqrt{d})$ is

- $\mathbb{Z}[\sqrt{d}]$ if $d \equiv 2, 3 \mod 4$
- $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ if $d \equiv 1 \mod 4$

Units in the ring of integers

<u>Definition</u>: For any "ring" R an element $r \in R$ is called a <u>unit</u> (aka <u>invertible</u>) if $\exists\, s \in R$ s.t. $rs = 1$.

<u>Example</u>: 1) Units in $\mathbb{Z}$ are $\{\pm 1\}$

2) Units in $\mathbb{Z}/n\mathbb{Z}$ are $\{a \in \mathbb{Z}/n\mathbb{Z} \mid GCD(a, n) = 1\}$

3) Units in $\mathrm{Mat}_{n\times n}(\mathbb{R})$ are

$$\{ A \in \mathrm{Mat}_{n\times n}(\mathbb{R}) \mid \det(A) \neq 0 \}$$

$$= GL_n(\mathbb{R})$$

4) Units in $\mathbb{Z}[i]$ are

$$\{ \pm 1, \pm i \}.$$

<u>Units in $\mathbb{Z}[\sqrt{d}]$</u>

Let $s + t\sqrt{d}$ be a unit in $\mathbb{Z}[\sqrt{d}]$.

Hence, $\exists$ s' and $t' \in \mathbb{Z}$ s.t.

$$(s + t\sqrt{d})(s' + t'\sqrt{d}) = 1$$

$$\Rightarrow (ss' + tt'd) + \sqrt{d}(st' + ts') = 1$$

$$\Rightarrow \quad ss' + tt'd = 1 \; ; \quad st' + ts' = 0$$

$$\begin{pmatrix} s & td \\ t & s \end{pmatrix} \begin{pmatrix} s' \\ t' \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

solvable in $\mathbb{Z}$ only if $\det \begin{pmatrix} s & td \\ t & s \end{pmatrix} \in \{\pm 1\}$

$$\Leftrightarrow s^2 - t^2 d = \pm 1.$$

<u>Prop</u>: Let $d \equiv 2$ or $3 \mod 4$ so that the integer ring of $\mathbb{Q}(\sqrt{d})$ is $\mathbb{Z}[\sqrt{d}]$. An element $a = s + t\sqrt{d}$ is a unit if and only if $|a\bar{a}| = 1$ where $\bar{a}$ is the conjugate of a given by $\bar{a} = s - t\sqrt{d}$. In other words $s^2 - t^2 d = \pm 1$, i.e. (s,t) solves the Pell's equation.

<u>Proof</u>: First note that for any

$$a = s + t\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$$

$$a\bar{a} = (s + t\sqrt{d})(s - t\sqrt{d}) = s^2 - t^2 d \in \mathbb{Z}$$

Let $b \in \mathbb{Z}[\sqrt{d}]$ s.t. $ab = 1$.

Thus $(ab)(\overline{ab}) = 1$

[check: $\overline{ab} = \bar{a}\,\bar{b}$]

$\Rightarrow (a\bar{a})(b\bar{b}) = 1$

Let $a\bar{a} = A$ and $b\bar{b} = B$, $A, B \in \mathbb{Z}$

But $AB = 1$ has only possible solutions (± 1).

Thus $A = \pm 1$

$$\Rightarrow \quad s^2 - d t^2 = \pm 1 .$$

Converse follows from the calculation before the Prop. $\boxtimes$

Exercise: What is the ring of integers of $\mathbb{Q}(5i)$

of $\mathbb{Q}(\sqrt{3})$

(check $d \equiv 1$ or $2, 3 \bmod 4$) of $\mathbb{Q}(\sqrt{14})$

of $\mathbb{Q}(\sqrt{7}\, i)$

Exercise: Calculate the units in the ring of integers of $\mathbb{Q}(\sqrt{26})$.

Exercise: Calculate the unit in the ring of integers of $\mathbb{Q}(\sqrt{97}\, i)$

Exercise: Let $d < 0$ and $d \equiv 2$ or $3 \bmod 4$. Find the units in $\mathbb{Z}[\sqrt{d}]$.