LECTURE 34

Dec. 10/2003.

Last time:

determined the ring of all algebraic integers in the field $\mathbb{Q}(\sqrt{d})$ (d squarefree integer):

$$R = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{d} & d \equiv 2,3 \pmod 4 \\ \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right) & d \equiv 1 \pmod 4 \end{cases}$$

There is also a uniform way of writing this. First define the <u>discriminant</u>

$$D = \begin{cases} 4d & , \quad d \equiv 2,3 \pmod 4 \\ d & , \quad d \equiv 1 \pmod 4 \end{cases}$$

Then infact: $R = \mathbb{Z} + \mathbb{Z}\left(\frac{D+\sqrt{D}}{2}\right)$.

When $D<0$ ($\Leftrightarrow d<0$), we call these "imaginary quadratic rings"

<u>Def'n</u> The <u>Norm map</u> $N : R \to \mathbb{Z}$ is defined by

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

Given $\alpha = a+b\sqrt{d}$ we often denote $\alpha' := a-b\sqrt{d}$ and call it the "<u>conjugate</u>" of α.

<u>Property of N:</u> $N(\alpha\beta) = N(\alpha)\cdot N(\beta)$.

Rmk When $d<0$ ($\Leftrightarrow D<0$) $N(\alpha)\geq 0$ for all $\alpha\in R$.

Prop α is a unit in $R \Leftrightarrow$ $N(\alpha)=\pm 1$ is a unit in $\mathbb{Z}$.

Pf) · If α is a unit, then $\exists\ \beta\in R$ s.t. $\alpha\beta=1$. Then
$N(\alpha\beta)=N(\alpha)\cdot N(\beta)=N(1)=1$.
Thus $N(\alpha)\in\mathbb{Z}^\times=\{\pm 1\}$

· Conversely, if $N(\alpha)=\pm 1$ then $\pm\alpha'$ is an inverse for α since $\alpha\alpha'=N(\alpha)$. $\boxtimes$

Cor If $D<0$ then α is a unit $\Leftrightarrow$ $N(\alpha)=+1$ (since when $d<0$, $N(\alpha)\geq 0\ \forall\alpha$)

Cor In fact, if $D=-3$, there are 6 units
if $D=-4$, there are 4 units
if $D<-4$, there are 2 units ($R^\times=\{\pm 1\}$)

Pf) A unit $\alpha=a+b\sqrt{d}$ is a solution to $a^2-b^2d=1$ where $a,b\in\mathbb{Z}$ or $a,b\in\frac{1}{2}\mathbb{Z}-\mathbb{Z}$ (according to case of d)

If $b=0$, $a^2=1$ so $a=\pm 1$ & $\alpha=\pm 1$.
If $b\neq 0$, then $-b^2d\geq -d/4$ ($|b|\geq\frac{1}{2}$)
so if $-d>4$ then can have any more solutions.
The cases $D=-3,-4$ are easy to verify directly. $\boxtimes$

Prop If $D>0$, $R^\times$ is infinite.

Example: $D=5$, $R=\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{5}}{2}\right)$

$\alpha=\frac{1+\sqrt{5}}{2}$; $\alpha\alpha'=-1 \Rightarrow$ $\alpha\in R^\times$ with $\alpha^{-1}=-\alpha'=\frac{-1+\sqrt{5}}{2}$.

Observe: writing $\alpha^n=a_n+b_n\sqrt{d}$ then the sequences (a_n), (b_n) are increasing (induction) so $\{\alpha^n : n\in\mathbb{Z}\}$ is an infinite subgroup of $R^\times$.

Ideal theory when $D<0$ of $R=$ ring of ints in $\mathbb{Q}(\sqrt{D})$

Saw previously:

$d=-1$, $\mathbb{Z}[i]$ is a Euclidean ring

However: If $d<-1$ & $d\equiv 3 \pmod 4$ then $R=\mathbb{Z}+\mathbb{Z}\sqrt{d}$ is not a unique factorization domain

$d=-5,-13,-17,-21,\ldots$

To prove this, consider:

$$1-d=(1+\sqrt{d})(1-\sqrt{d})=2\cdot\frac{(1-d)}{2}$$

Claim 2 is an irreducible element in R

Pf) Suppose $2=\alpha\beta$ with neither α nor β a unit. Then $N(2)=4=N(\alpha)N(\beta)$

$\Rightarrow N(\alpha)=N(\beta)=2$

This is impossible since if $\alpha = a+b\sqrt{d}$, $a, b' \in \mathbb{Z}$ (since $d \equiv 3 \bmod 4$)

then $N(\alpha) = a^2 - db^2$

& $d \leq -5 \Rightarrow b = 0$

$\Rightarrow a^2 = 2$ which is contradiction $\boxtimes$

However $2 \nmid (1+\sqrt{d})$ so have distinct factorization.

It follows that not every ideal in R is principal.

Although not all ideals $I \subset R$ are principal, every I can be generated by 2 elements $I = (\alpha, \beta)$.

Why? Either $I = (0)$, or I has finite index in R (i.e. R/I is finite).

To see this: If $\alpha \neq 0$ in I, then $N(\alpha) = \alpha\alpha' = n > 0$ is also in I, so $\underbrace{(n) \subset I \subset R}_{n^2} = \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right)$

so $[R : I] \leq n^2$

(cf. argument when $d = -1$).

$R \subset \mathbb{C}$ is a discrete subgroup of $(\mathbb{C}, +)$, stable under mult.
$I \subset \mathbb{C}$ is a smaller such subgroup, stable under mult. by R

→ Note: this last condition of stab. under mult. by R is equiv. to being stable under mult. by $\frac{D+\sqrt{D}}{2}$.

Note: Can draw pictures of I & R.

Any subgroup of R of finite index can be generated (as a subgroup) by 2 elements (cf. our classification of lattices in $\mathbb{R}^2$). Thus we can find α, β that generate I. $\boxtimes$