# LECTURE 36

Dec. 15/03

$D<0$ some discriminant
$R_D = \mathbb{Z} + \mathbb{Z}\left(\frac{D+\sqrt{D}}{2}\right) \subseteq \mathbb{C}$
is lattice
$0 \neq I \subset R_D$
$\uparrow$ finite index automatically;
$(R_D : I) = N \cdot I$ ~~where~~ $N =$ norm $\geq 1$

e.g.: if $I = \alpha R_D$ for some $\alpha \neq 0$ in $R_D$, then $N = \alpha\bar{\alpha}$

Question: How far is $R_D$ from being a principal ideal domain?

Def'n A fractional ideal $I \subset \mathbb{Q}(\sqrt{D})$ (= field of fractions of $R_D$) is a lattice in $\mathbb{C}$ (in particular a subgroup; also discrete) which is stable under multiplication by $R_D$.

- For example, if $\beta \in \mathbb{Q}(\sqrt{D})$ and $\beta \neq 0$ then $I = \beta R_D$ is a fractional ideal for $R_D$. Also any ideal $I$ of $R_D$ is a fractional ideal.
- Multiplication of ideals generalizes to multiplication of fractional ideals

$$I \cdot J = J \cdot I = \left\{ \sum_{1}^{n} a_i b_i : \begin{array}{l} n \text{ not fixed} \\ a_i \in I,\ b_i \in J \end{array} \right\}$$

e.g.: $(\alpha R_D)\cdot(\beta R_D) = (\alpha\beta)R_D$.

Proposition (Kummer, Dedekind)

① The fractional ideals form an (infinite) abelian group under multiplication, with identity the ideal $R=(1)$.

② The principal ideals form a subgroup.

③ The quotient group

$$C_D := \frac{\{\text{fractional ideals}\}}{\{\text{principal ideals}\}}.$$

which is called the ideal class group. is a finite group.

$$h_D := \text{order of the ideal class group } C_D.$$

- Various mathematicians calculated $h_D$ for discriminants $D<0$ and found that (experimentally)
  - they could get $h_D = 1$ for $D < -163$
  - $h_D \approx |D|^{1/2}$

It is known that $\exists c$ s.t.

$$h_D < c|D|^{1/2} \log|D|$$

It is expected that $\exists c'$ s.t.

$$\frac{c'|D|^{1/2}}{\log|D|} < h_D$$

but this is unkown & linked to Riemann hyp.

**Rmk:** Given $I \subset \mathbb{Q}(\sqrt{D})$ fractional ideal there is $N$ s.t. $NI \subset R_D$. Thus every coset in $C_D$ is represented by an ideal of $R_D$ (not just a fractional ideal).

---

Amazingly enough: all of this is related to analysis.

Euler: $\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ primes}} \left(1 - \frac{1}{p^s}\right)^{-1}$

$\left( = \prod_{p \text{ primes}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right)\right)$

$s > 1$

Cor $\sum_{p \text{ prime}} \frac{1}{p}$ does not converge ($= \infty$)

Dirichlet (1837):

$$\zeta_D(s) := \sum_{\substack{(0) \neq I \subseteq R_D \\ \text{nonzero ideal}}} \frac{1}{(NI)^s} = \sum_{\mathfrak{P} \text{ prime ideals}} \left(1 - \frac{1}{(N\mathfrak{P})^s}\right)^{-1}$$

(where $NI = (R_D : I)$)

(unique fact. into prime ideals) $\rightarrow$ saw this last time.

$s > 1$

$\left[\text{and } I = \mathfrak{P}_1 \cdots \mathfrak{P}_k \Rightarrow NI = (N\mathfrak{P}_1) \cdots (N\mathfrak{P}_k)\right]$

**Prop**

Suppose $p$ is a rational prime. Then either

① $pR$ is a prime ideal
$\mathbb{N}(pR) = p^2$

② There are two distinct prime ideals $\underline{P}, \underline{P}'$

$$pR \subset \underline{P} \subset R_D, \quad pR \subset \underline{P}' \subset R_D$$

s.t. $\underline{P}\,\underline{P}' = pR$ &

$$\mathbb{N}(\underline{P}) = \mathbb{N}(\underline{P}') = p$$

③ There is a unique prime ideal

$$pR \subset \underline{P} \subset R$$

$$\mathbb{N}(\underline{P}) = p \quad \& \quad \underline{P}^2 = pR$$

e.g. if $R_D = \mathbb{Z}[i]$ then we are in case ① if $p \equiv 3 \pmod 4$

② if $p \equiv 1 \pmod 4$

③ if $p = 2$.

Thus

$$\zeta_{R_D}(s) = \prod_{p \text{ in case ①}} \left(1 - \frac{1}{p^s}\right)^{-1} \left(1 + \frac{1}{p^s}\right)^{+1}$$

$$\cdot \prod_{p \text{ in case ②}} \left(1 - \frac{1}{p^s}\right)^{-1} \left(1 - \frac{1}{p^s}\right)^{-1}$$

$$\cdot \prod_{p \text{ in case ③}} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

Hence $\zeta_{R_D}(s) = L_D(s) \cdot \zeta(s)$

where $L_D(s) = \prod_{p \text{ in case } ①} \left(1+\frac{1}{p^s}\right)^{-1} \cdot \prod_{p \text{ in case } ②} \left(1-\frac{1}{p^s}\right)^{-1}$

- For example, for $\mathbb{Z}[i]$:

$$L_{-4}(s) = \prod_{p\equiv 1 \pmod 4} \left(1-\frac{1}{p^s}\right)^{-1} \cdot \prod_{p\equiv 3 \pmod 4} \left(1+\frac{1}{p^s}\right)^{+1}.$$

$$= \sum_{\substack{n\geq 1\\ \text{odd}}} \frac{\pm 1}{n^s} \quad \left\{ \text{where } \begin{array}{l} +1 \text{ if } n\equiv 3 \pmod 4 \\ -1 \text{ if } n \equiv 1 \pmod 4 \end{array} \right.$$

$\boxed{\text{Note: } L_{-4}(1) = \pi/4 \text{ converges}}$

## Dirichlet class # formula

$$L_D(1) = \frac{2\pi}{\sqrt{|D|}} \cdot \frac{h_D}{\# R_D^\times} > 0.$$

- For example:

for $D=-4$

$$\frac{\pi}{4} = \frac{2\pi}{\sqrt{4}} \cdot \frac{h_D}{4}$$

$\Rightarrow h_D = 1$ (which we knew already).

Thus to get asymptotic information about $h_D$, we want to show something about $L_D(1)$ as $D \to -\infty$:

e.g. if $L_D(1) \approx 1$ then $h_D \approx |D|^{1/2}$.

Relation to Riemann hypothesis:
RH controls size of $J_{R_D}$ near 1.