Lecture 35

Friday, April 3, 2015 10:05 AM

D a square-free integer $(n^2 \nmid D)$

$\mathbb{Q}(\sqrt{D}) = \{ a + b\sqrt{D} \mid a, b \in \mathbb{Q} \}$

$\cup\!\!|$ field

$\mathcal{O} = \mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \mathbb{Z}[\omega] = \{ a + b\omega \mid a, b \in \mathbb{Z} \}$

for $\omega = \begin{cases} \sqrt{D} & \text{if } D \equiv 2, 3 \ (4) \\ \frac{1+\sqrt{D}}{2} & \text{if } D \equiv 1 \ (4) \end{cases}$

ring, in fact an integral domain

Field norm $N : \mathbb{Q}(\sqrt{D}) \longrightarrow \mathbb{Q}$

$$a + b \cdot \sqrt{D} \longmapsto (a + b\sqrt{D})(a - b\sqrt{D})$$
$$= a^2 - Db^2$$

Note: $D = -1$, $\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \mathbb{Z}[i]$

$$N : \mathbb{Q}(\sqrt{-1}) \longrightarrow \mathbb{Q}$$
$$a + bi \longmapsto a^2 + b^2 = |a+bi|^2$$

Check N is multiplicative: $N(\alpha\beta) = N(\alpha)N(\beta)$.

$$\bar{\omega} = \begin{cases} -\sqrt{D} & D \equiv 2,3\ (4) \\ \frac{1-\sqrt{D}}{2} & \text{if } D \equiv 1\ (4) \end{cases}$$

Restrict to $\mathcal{O}$:

$a+b\omega \in \mathcal{O}$, $a, b \in \mathbb{Z}$ then

$$N(a+b\omega) = (a+b\omega)(a+b\bar{\omega})$$

$$= \begin{cases} a^2 - Db^2 & D \equiv 2,3\ (4) \\ a^2+ab+\frac{1-D}{4}b^2 & D \equiv 1\ (4). \end{cases}$$

$\in \mathbb{Z}$

I.e. $N : \mathcal{O} \longrightarrow \mathbb{Z}$.

If $\underset{a+b\omega}{\overset{\shortparallel}{\alpha}} \in \mathcal{O}$ & $N(\alpha) = \pm 1$, then $\alpha^{-1} = \pm(a+b\bar{\omega}) \in \mathcal{O}$

so $\alpha \in \mathcal{O}^\times$. If $\alpha\beta = 1$ (for $\alpha, \beta \in \mathcal{O}$) then $N(\alpha)N(\beta) = 1$

$\Rightarrow N(\alpha) \in \mathbb{Z}^\times = \{\pm 1\}$.

<u>Moral</u> $\mathcal{O}^\times = N^{-1}(\pm 1) = \{\alpha \in \mathcal{O} \mid N(\alpha) = \pm 1\}$.

Friday, April 3, 2015 10:17 AM

Q What are the irreducibles in $\mathcal{O}$?

Suppose $\alpha \in \mathcal{O}$ w/ $N(\alpha) = p$ a prime in $\mathbb{Z}$.

If $\alpha = \beta\gamma$, $\beta, \gamma \in \mathcal{O}$ then $p = N(\beta)N(\gamma)$

$\Longrightarrow N(\beta)$ or $N(\gamma) = \pm 1 \Longrightarrow \beta$ or $\gamma \in \mathcal{O}^\times$

$\Longrightarrow \alpha$ is irreducible in $\mathcal{O}$.

If π is prime in $\mathcal{O}$ then $(\pi) \cap \mathbb{Z}$ is a prime ideal, say $(\pi) \cap \mathbb{Z} = (p)$. If $\pi = a + b\omega$, $a, b \in \mathbb{Z}$, then $N(\pi) = \pi(a + b\bar{\omega}) \in (\pi) \cap \mathbb{Z} = (p)$

Thus $p \in (\pi)$ & $\pi \mid p$ in $\mathcal{O}$.

<u>Moral</u> To find primes in $\mathcal{O}$, find divisors in $\mathcal{O}$ of each rational prime p.

If $p = \pi\pi'$, then $p^2 = N(\pi)N(\pi') \Longrightarrow$

$N(\pi) = \pm p^2$ or $\pm p$.

If $N(\pi) = \pm p^2$, then $N(\pi') = 1 \Longrightarrow \pi' \in \mathcal{O}^\times$

$\Longrightarrow \pi$ is an associate of p which is irreducible in $\mathcal{O}$.

Friday, April 3, 2015 10:26 AM

If $p = \pi\pi'$ & $N(\pi) = \pm p = N(\pi')$, then π, π' are irreducible.

Specialize to $D = -1$

Then $\mathcal{O} = \mathbb{Z}[i]$ is a Euclidean domain and thus a UFD.

So primes = irreducibles in $\mathbb{Z}[i]$.

<u>Goal</u> Factor rat'l primes $p \in \mathbb{Z}$ in $\mathbb{Z}[i]$, to get primes in $\mathbb{Z}[i]$.

$$N(a+bi) = a^2 + b^2 = (a+bi)\overline{(a+bi)}$$

p factors in $\mathbb{Z}[i]$ into 2 irreducibles $\iff$ $p = a^2 + b^2$, i.e. p is a sum of square integers.

O/w p is irreducible in $\mathbb{Z}[i]$.

e.g. $2 = 1^2 + 1^2$ so $1+i$ & $1-i$ are irreducible in $\mathbb{Z}[i]$

$\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ and $1-i = -i(1+i)$

If $p = a^2+b^2$ then $p = (a+bi)(a-bi)$

not associate unless $p=2$.

Observe: $n^2 \equiv 0$ or 1 (4) $\forall n \in \mathbb{Z}$.

Thus $a^2+b^2 \equiv (0 \text{ or } 1) + (0 \text{ or } 1) \quad (4)$

$\equiv 0, 1, \text{ or } 2 \quad (4)$.

Thus if $p \equiv 3$ (4), then $p \neq a^2+b^2$ $\forall a,b \in \mathbb{Z}$.

Thus if $p \equiv 3$ (4), then p is irreducible in $\mathbb{Z}[i]$.

What if $p \equiv 1$ (4)?

<u>Lemma</u> A prime $p \in \mathbb{Z}$ divides some integer n^2+1 for some $n \in \mathbb{Z}$ iff $p=2$ or $p \equiv 1$ (4).

Pf Easy if we know $(\mathbb{Z}/p\mathbb{Z})^\times \cong C_{p-1}$ ...

By the lemma, if $p \equiv 1$ (4) is prime, then $p \mid n^2+1$ in $\mathbb{Z}$ for some $n \in \mathbb{Z}$.

Thus $p \mid (n+i)(n-i)$ in $\mathbb{Z}[i]$.

If p is irreducible in $\mathbb{Z}[i]$, then

$p \mid n+i$ or $p \mid n-i$.

$$pz = n+i \iff \overline{pz} = n-i \implies p \mid \underbrace{(n+i)-(n-i)}_{=2i}$$

$$\overline{pz} = p\bar{z}$$

By multiplicativity of norm, this is absurd, ☠.

Thus p is reducible in $\mathbb{Z}[i]$. $\square$

<u>Fermat's thm on sums of $\square$s</u>

$p = a^2+b^2$ for some $a, b \in \mathbb{Z} \iff p = 2$ or $p \equiv 1$ (4).