# Lecture 47

(47.0) Recall: a <u>Euclidean domain</u> is an integral domain $R$ such that there exists a function

$$N : R \longrightarrow \mathbb{Z}_{\geq 0} \qquad (N(0) = 0)$$

such that: for every $a, b \in R$; $b \neq 0$, we can find $q, r \in R$ so that
- $a = qb + r$; and
- $N(r) < N(b)$; or $r = 0$.

Our usual examples (from Lecture 35):

$R = \mathbb{Z}$; $N(\ell) = |\ell| \quad \forall\ \ell \in \mathbb{Z}$

$R = K[x]$; $N(f(x)) =$ degree of $f(x)$ $\forall\ f(x) \in K[x]$

($K$ a field)

$R = \mathbb{Z}[\sqrt{-1}]$; $N(a + b\sqrt{-1}) = a^2 + b^2$ $\forall\ a, b \in \mathbb{Z}$.

(47.1) As we proved in Lecture 35; all these examples are P.I.D.'s — and the same proof works for any Euclidean domain.

**Lemma:** Let $R$ be a Euclidean domain. Then $R$ is a principal ideal domain.

**Proof:** Let $N : R \longrightarrow \mathbb{Z}_{\geq 0}$ be as promised by the definition of a Euclidean domain.

Let $I \subsetneq R$ ; $I \neq (0)$ be a non-zero ideal

Choose $b \in I \setminus \{0\}$ of smallest $N$.

Claim : $I = (b)$

Proof. For $a \in I$; write $a = qb + r$. We find so that $N(r) < N(b)$ or $r = 0$

that, by our choice of $b$, $r = 0$ is the only option.

Hence $I = (b) \subseteq I$ .

(because $b \in I$)

□

(47.2) Source of examples - quadratic integer rings.

$\mathbb{C} \supset \mathbb{Q}(\sqrt{D})$ ; $D \in \mathbb{Z} \setminus \{0, 1\}$

$\sqrt{D} \notin \mathbb{Z}$

$\mathbb{C}$ = field of complex numbers

$\mathbb{Q}(\sqrt{D})$ = Smallest subfield of $\mathbb{C}$ containing $\sqrt{D} \in \mathbb{C}$

Infact we will assume that $D$ is square-free

(i.e. $D = \pm p_1 p_2 \cdots p_\ell$ for $p_1, \ldots, p_\ell \in \mathbb{Z}_{\geq 2}$ distinct primes)

Subring $\mathcal{O}(\sqrt{D}) \subset \mathbb{Q}(\sqrt{D})$ is defined by:

Let $\mathbb{Q}(\sqrt{D}) \xrightarrow{N} \mathbb{Q}$

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

$$\mathcal{O}(\sqrt{D}) := \{ x \in \mathbb{Q}(\sqrt{D}) \mid N(x) \in \mathbb{Z} \}$$

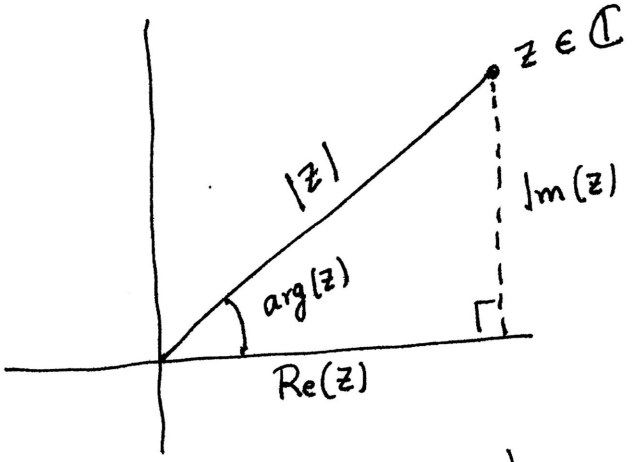
Exercise: $\mathcal{O}(\sqrt{D}) = \mathbb{Z} + \mathbb{Z}\omega =: \mathbb{Z}[\omega]$

$$= \{ a+b\omega \mid a \in \mathbb{Z},\ b \in \mathbb{Z} \}$$

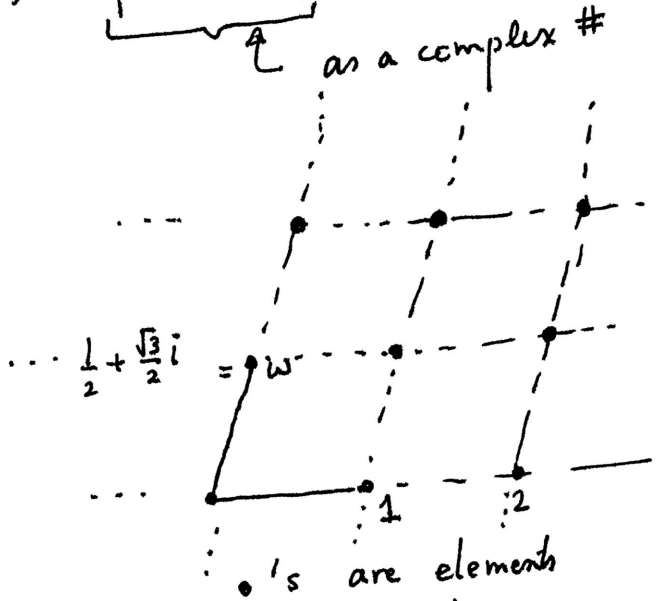
$\omega = \frac{1+\sqrt{D}}{2}$ if $D \equiv 1 \bmod 4$

$= \sqrt{D}$ if $D \equiv 2,3 \bmod 4$

e.g. $D < 0 \Rightarrow N(a+b\sqrt{D}) = \underbrace{|a+b\sqrt{D}|^2}_{\text{as a complex \#}}$




$(-\pi < \arg(z) \leq \pi)$




•'s are elements of $\mathcal{O}(\sqrt{-3})$

$\mathcal{O}(\sqrt{-3})$ for example

(47.3) Revisiting - how we proved $\mathbb{Z}[\sqrt{-1}]$ is Euclidean: -

Take $D = -2$ (same argument works)

$$\mathcal{O}(\sqrt{-2}) = \{ z = a + \sqrt{2}bi \in \mathbb{C} \mid a, b \in \mathbb{Z} \} \subset \mathbb{Q}(\sqrt{-2})$$

$$= \mathbb{Z}[\sqrt{-2}]$$

$$N = |\cdot|^2 : \mathbb{Z}[\sqrt{-2}] \longrightarrow \mathbb{Z}_{\geq 0}$$

Euclidean property: given $\alpha, \beta \in \mathbb{Z}[\sqrt{-2}]$, say $\beta \neq 0$,

write $\frac{\alpha}{\beta} \in \mathbb{Q}(\sqrt{-2})$ as $\frac{\alpha}{\beta} = \rho_1 + \rho_2\sqrt{-2}$.

Up to shifts by elements of $\mathbb{Z}[\sqrt{-2}]$, we may assume

$-\frac{1}{2} \leq \rho_1, \rho_2 \leq \frac{1}{2}$. i.e. $\exists\ \gamma \in \mathbb{Z}[\sqrt{-2}]$ s.t.

$$\left| \frac{\alpha}{\beta} - \gamma \right|^2 \leq \frac{1}{4} + \frac{2}{4} < 1$$

$\Rightarrow \quad \alpha = \beta \cdot \gamma + r$ where either $|r|^2 < |\beta|^2$

Note: for $N(\alpha) = |\alpha|^2$, we already know

- $N(r) = 0 \iff r = 0$.
- $N(\alpha_1 \cdot \alpha_2) = N(\alpha_1) \cdot N(\alpha_2)$

Hence $\alpha \in (\mathbb{Z}[\sqrt{-2}])^\times \Rightarrow N(\alpha) = |\alpha|^2 = 1 \Rightarrow \alpha = \pm 1$.

(47.4) Take $D = -3$.

$$\mathcal{O}(\sqrt{-3}) = \mathbb{Z}[\omega] \quad \text{where } \omega = \frac{1}{2} + \frac{\sqrt{-3}}{2}$$

Same trick as before $N: \mathbb{Z}[\omega] \longrightarrow \mathbb{Z}_{\geq 0}$

$$\begin{array}{ccc} \cap & & \cap \\ \mathbb{C} & \longrightarrow & \mathbb{R}_{\geq 0} \\ \wr & & \wr \\ z & \longmapsto & |z|^2 \end{array}$$

Let $\alpha, \beta \in \mathbb{Z}[\omega]$ ; $\beta \neq 0$. Again, write

$$\frac{\alpha}{\beta} = p_1 + p_2 \cdot \sqrt{-3} \quad ; \quad p_1, p_2 \in \mathbb{Q}.$$

Shifts are allowed by $a + b\left(\frac{1}{2} + \frac{\sqrt{-3}}{2}\right)$

i.e. $a + \frac{b}{2} + \frac{b}{2}\sqrt{-3}$.

So we may assume $-\frac{1}{4} \leq p_2 \leq \frac{1}{4}$ and $-\frac{1}{2} \leq p_1 \leq \frac{1}{2}$.

i.e. $\exists\ \gamma \in \mathbb{Z}[\omega]$, s.t. $\left|\frac{\alpha}{\beta} - \gamma\right|^2 \leq \frac{1}{4} + \frac{3}{16} = \frac{7}{16} < 1$

i.e. $\alpha = \beta \cdot \gamma + r$ where $|r|^2 < |\beta|^2$ ✓.

Same argument works for $D = -7, -11$ e.g. [Ex.]
(these are $\equiv 1 \bmod 4$)

(47.5) $D = -5$. $\mathcal{O}(\sqrt{-5}) = \mathbb{Z} + \mathbb{Z}\sqrt{-5} = \mathbb{Z}[\sqrt{-5}]$ (say $\xi$).

$|a + b\xi|^2 = a^2 + 5b^2$ — this argument fails.

In fact $\mathbb{Z}[\sqrt{-5}]$ is not even a principal ideal domain

Claim : $I = (3, 2+\sqrt{-5}) \subset R = \mathbb{Z}[\sqrt{-5}]$ is not a principal ideal.

Proof : Assume there exists $\alpha \in R$ such that $I = (\alpha)$.

Then $3 \in (\alpha) \Rightarrow 3 = \alpha\beta$ for some $\beta \in R$.

$\Rightarrow |3|^2 = |\alpha|^2 |\beta|^2$ i.e. $|\alpha|^2 \cdot |\beta|^2 = 9$.

As $|\alpha|^2 = a^2 + 5b^2$ we know $|\alpha|^2$ cannot be 3.

(if $\alpha = a + \sqrt{-5}\, b$ $a, b \in \mathbb{Z}$)

Option A. $|\alpha|^2 = 9$. In this case $|\beta|^2 = 1 \Rightarrow \beta = \pm 1$.

That is $3 = \pm\alpha$ i.e. $(3, 2+\sqrt{-5}) = (3)$. But this means $2 + \sqrt{-5} = 3(m + n\sqrt{-5})$ for some $m, n \in \mathbb{Z}$.

But this is impossible.

Option B. $|\alpha|^2 = 1$. That is, $\alpha = \pm 1$ and hence $I = R$.

Meaning $1 \in (3, 2+\sqrt{-5})$. So we can write :

$1 = 3 \cdot \gamma + (2+\sqrt{-5}) \cdot \delta$ for some $\gamma, \delta \in R$.

$\Rightarrow (2 - \sqrt{-5}) = 3 \cdot \gamma \cdot (2 - \sqrt{-5}) + 9 \cdot \delta$

$= 3(m + n\sqrt{-5})$ for some $m, n \in \mathbb{Z}$.

This is again impossible. □