Lecture 48

(48.0) Recall: we worked out some examples of rings of quadratic integers.

$D =$	-1	-2	-3	-5	$\cdots$	-19
$\omega =$	$\sqrt{-1}$	$\sqrt{-2}$	$\frac{1}{2}+\frac{\sqrt{-3}}{2}$	$\sqrt{-5}$	$\cdots$	$\frac{1}{2}+\frac{\sqrt{-19}}{2}$
$\mathcal{O}(\sqrt{D}) = \mathbb{Z}[\omega]$ $\cap$ $\mathbb{Q}(\sqrt{-D}) \subset \mathbb{C}$	Euclidean (hence PID)	Euclidean (hence PID)	Euclidean (hence PID)	Not PID (hence not Euclidean)	$\cdots$	Not Euclidean but PID

Example: $D = -19$.

Let $\omega = \frac{1}{2} + \frac{\sqrt{-19}}{2}$; $R = \mathbb{Z}[\omega]$ is not Euclidean.

We begin by assuming that R is Euclidean with respect to some function $\mathcal{N} : R \longrightarrow \mathbb{Z}_{\geq 0}$.

(Ex.) R is not a field. (Hint: $\omega \in R$ is not invertible
$$\mathbb{C} \ni \omega^{-1} = \frac{1}{|\omega|^2} \cdot \overline{\omega} = \frac{1}{(\sqrt{5})^2}\left(\frac{1}{2} - \frac{\sqrt{-19}}{2}\right) \notin R.)$$

So, the set $X = \{a \in R \mid a \neq 0,\ a \notin R^\times\} \neq \phi$.

Let $u \in X$ be so that $\mathcal{N}(u)$ is smallest.

Thus for any $x \in R$, Euclidean property of $N: R \to \mathbb{Z}_{\geq 0}$ implies $x = qu + r$ where $N(r) < N(u)$

as $u \in X$ has smallest $N(\cdot)$ among all elements of X, we conclude that $r = 0$ or $r \in R^{\times}$.

Claim: There is no such $u \in R$. - we are heading towards a contradiction.

[Recall: we still have

$$R = \mathbb{Z}[\omega] \longrightarrow \mathbb{Z}_{\geq 0}$$
$$\alpha \longmapsto |\alpha|^2 \text{ as complex \#'s}$$

so $\alpha \in R^{\times} \Rightarrow \alpha \cdot \beta = 1$ for some $\beta \in R$ $\Rightarrow |\alpha|^2 (\cdot |\beta|^2) = 1$.

Now $\alpha = a + b\omega \Rightarrow |\alpha|^2 = \left(a + \frac{b}{2}\right)^2 + \frac{19}{4} \cdot b^2$. So

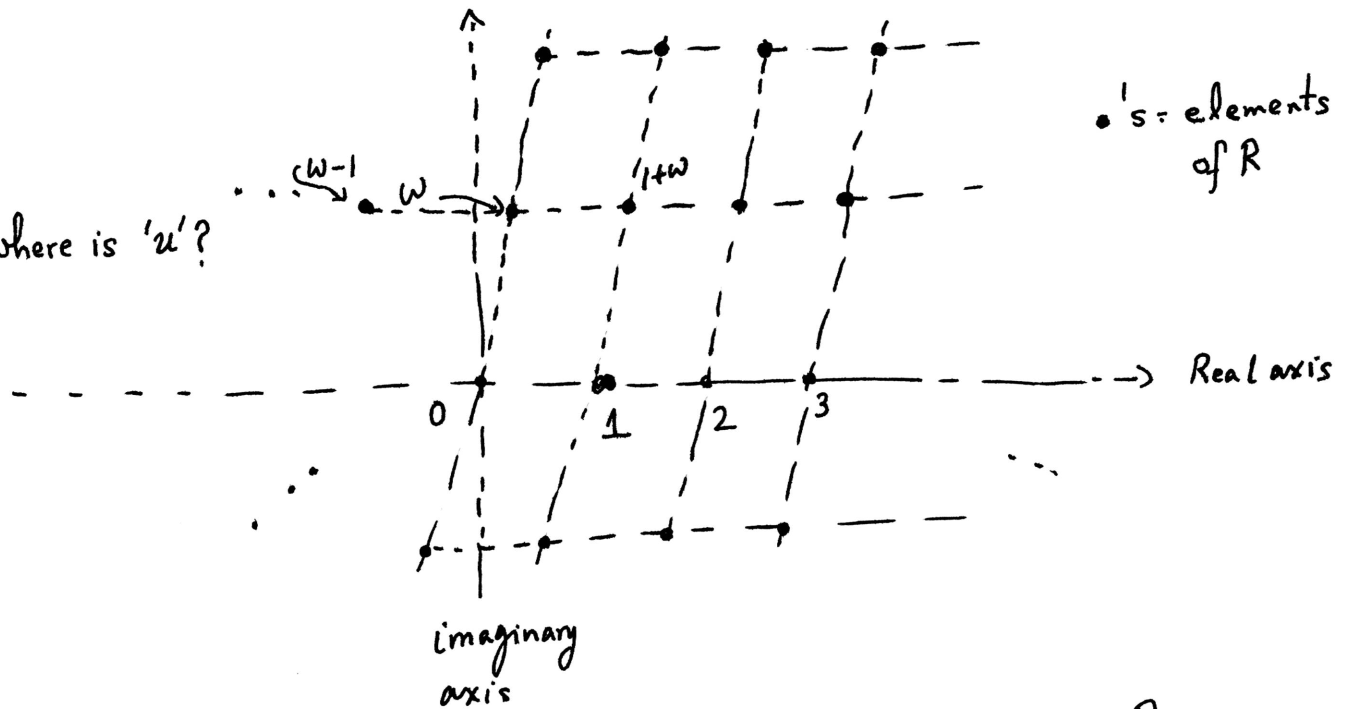
$|\alpha|^2 = 1 \iff \alpha = \pm 1$; i.e. $\boxed{R^{\times} = \{\pm 1\}}$.]

As noticed above; for our $u \in R$; $\forall x \in R$, $\exists r \in \{0, +1, -1\}$ such that u divides $x - r$. — (*)

Take $x = 2 \in R$. we must have: u divides 2, 1 or 3.

we assumed u is not a unit; so it is not going to divide 1.

Picture of $\mathbb{Z}[\omega]$; $\omega = \frac{1}{2} + \frac{\sqrt{-19}}{2}$ $\left(|\omega|^2 = 5\right)$



Q: where is 'u'?

Case 1 u divides 2 i.e. $2 = u \cdot v$ for some $v \in R$

$\Rightarrow |u|^2 \cdot |v|^2 = 4$. $\boxed{\text{Since } |u|^2 \geq 5 \text{ if } \mathrm{Im}(u) \neq 0 \text{ and } u \neq \pm 1}$

we must have

$|u|^2 = 4$; $|v|^2 = 1$ i.e $u = \pm 2$.

Say $u = 2$. Then take $x = \omega$ in (*) and note that

$$|\omega|^2 = |\omega - 1|^2 = 5 \quad ; \quad |\omega + 1|^2 = 7 \quad \text{all primes!}$$

$\Rightarrow$ $u = 2$ cannot divide ω, $\omega - 1$ or $\omega + 1$. Contradiction

Case 2 u divides 3 i.e. $3 = u \cdot v$ for some $v \in R$.

$\Rightarrow |u|^2 \cdot |v|^2 = 9$. Same argument as in

implies $|u|^2 = 9$; $|v|^2 = 1$ $\Rightarrow$ $u = \pm 3$.

Still cannot divide ω, $\omega + 1$ or $\omega - 1$. Contradiction. $\square$

(48.1) $\mathbb{Z}[\omega]$; $\omega = \frac{1}{2} + \frac{\sqrt{-19}}{2}$ is however a P.I.D.

[read Example on page 282 of our text book.]

Thus, we have strict inclusions:

$$\begin{array}{ccccccc}
\text{Fields} & \underset{(*)}{\subsetneq} & \text{Euclidean domains} & \subsetneq & \text{Principal ideal domains.} & \left(\subsetneq\right. & \left.\text{all Noetherian domains}\right). \\
\not\ni & & \ni & \not\ni & \ni & \not\ni & \ni \\
\mathbb{Z} & & \mathbb{Z} & \mathbb{Z}\left[\frac{1}{2}+\frac{\sqrt{-19}}{2}\right] & \mathbb{Z}\left[\frac{1}{2}+\frac{\sqrt{-19}}{2}\right] & & \mathbb{Z}[x] \\
 & & & & & & \mathbb{Z}[\sqrt{-5}] \\
 & & & & & & K[x,y]\ldots
\end{array}$$

(48.2) Recall - from Lecture 46 - for R = a principal ideal domain we have

(1) For every non-zero, proper ideal $I \subsetneq R$; there exist unique (non-zero) prime ideals $P_1, \ldots, P_\ell \subsetneq R$; $k_1, \ldots, k_\ell \geq 1$

s.t. $\quad I = P_1^{k_1} \cdots P_\ell^{k_\ell}$

(2) [Apply - every ideal is principal.]

$\forall\, n \in R$; $n \neq 0$, $n \notin R^\times$; $\exists\, p_1, \ldots, p_\ell \in R$
$\exists!\, k_1, \ldots, k_\ell \geq 1$

s.t. $\quad n = u \cdot p_1^{k_1} \cdots p_\ell^{k_\ell}$ for some $u \in R^\times$

[$p_1, \ldots, p_\ell \in R$ generate prime ideals in R - which are uniquely determined by n – i.e. $p_1, \dots, p_\ell \in R$ are uniquely determined by n – up to scaling by units.

Property (1) & (2) for PID's are equivalent to each other

can be generalized to "Dedekind domains"
[Noetherian domain where each non-zero prime ideal is maximal]

can be generalized to "UFD = unique factorization domains"
[defined below]

(48.3) Unique Factorization Domains.

Let R be a (Noetherian) integral domain.

- $a \in R$ is said to be an irreducible element if $a \neq 0$, $a \notin R^\times$ and for any $x, y \in R$; if $a = x.y$, then either x or y is a unit.

- $a \in R$ is said to be a prime element if $0 \neq (a) \subsetneq R$ is a prime ideal.
  (i.e. $x.y \in (a) \Rightarrow x \in (a)$ or $y \in (a)$.)

We say R is a unique factorization domain (UFD for short) if for every $n \in R$; $n \neq 0$; $n \notin R^\times$ we have

(i) n can be written as a (finite) product of irreducible elements (not necessarily distinct); $p_1, \ldots, p_m \in R$.

$$n = p_1 p_2 \cdots p_m$$

(ii) if $n = q_1 q_2 \cdots q_\ell$ for $q_1, \ldots, q_\ell \in R$ irreducible elements, then $m = \ell$ and, up to permutation, q's are related to p's by units of R. Meaning: there exists $\sigma \in S_m$ (permutation) and units $u_1, \ldots, u_m \in R^\times$ s.t $\boxed{u_i q_i = p_{\sigma(i)}}$ for each $i \in \{1, \ldots, m\}$

Lectures 45 and 46 were devoted to proving -

Theorem : Every P.I.D. is a U.F.D.

(48.4) Example : $R = \mathbb{Z}[\sqrt{-5}] \longrightarrow \mathbb{Z}_{\geq 0}$

$$z = a + b\sqrt{-5} \longmapsto |z|^2 = a^2 + 5b^2.$$

Claim : $3 \in R$ is an irreducible element but not a prime element

Pf. Assume $3 = \alpha \cdot \beta$ for some $\alpha, \beta \in R$.

Then $|\alpha|^2 \cdot |\beta|^2 = 9. \implies |\alpha|^2 = 1$ or $|\beta|^2 = 1$ or $|\alpha|^2 = 3 = |\beta|^2$

But $|\alpha|^2 = a^2 + 5b^2 \geq 5$ if $\mathrm{Im}(\alpha) \neq 0$

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

So $|\alpha|^2 = 3 = |\beta|^2$ is impossible. Hence $|\alpha|^2 = 1$ or $|\beta|^2 = 1$

i.e. either $\alpha = \pm 1$ is a unit.

or $\cancel{\alpha}\ \beta = \pm 1$ " " "

Now we show that $(3) \subset \mathbb{Z}[\sqrt{-5}]$ is not a prime ideal.

This is because $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 \in (3)$

but $1 \pm \sqrt{-5} \notin (3)$ since if $1 + \sqrt{-5} \in (3)$ then

there must exist integers $a, b \in \mathbb{Z}$ so that $1 + \sqrt{-5} = 3 \cdot (a + b\sqrt{-5})$

but that is absurd. $\square$