R : commutative integral domain

R is said to be euclidean if $\exists\ N : R \longrightarrow \mathbb{Z}_{\geq 0}$ s.t.

$\forall\ a, b \in R$ w/ $b \neq 0$, $\exists\ q, r$ s.t. $a = qb + r$

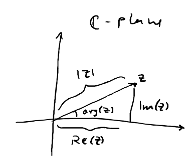
where $N(r) < N(b)$ or $r = 0$.

Lemma (Lecture 35 – $R = \mathbb{Z}$; $\mathbb{C}[x]$; $\mathbb{Z}[\sqrt{-1}]$): if R is euclidean then R is P.I.D.

Pf Let $\underset{\text{ideal}}{I \subset R}$, $I \neq (0)$. pick $b \in I \setminus \{0\}$ with smallest $N(b)$.

Claim: $I = (b)$. for any $a \in I$, $a = qb + r \Rightarrow r \in I$ with smaller $N(r) < N(b)$ if $r \neq 0$. $\square$

Examples: Rings of Quadratic integers.



$\mathbb{C} \supset \mathbb{Q}[\sqrt{D}]$ $\quad D \in \mathbb{Z}$, $D \neq 0, 1$

D is square-free

subfield of $\mathbb{C}$ containing $\sqrt{D}$

$\mathbb{Q}[\sqrt{D}] = \{p + q\sqrt{D} : p, q \in \mathbb{Q}\}$ $\quad D = \pm p_1 p_2 \cdots p_\ell$ $\quad$ ($p_i \in \mathbb{Z}_{\geq 2}$ distinct primes)

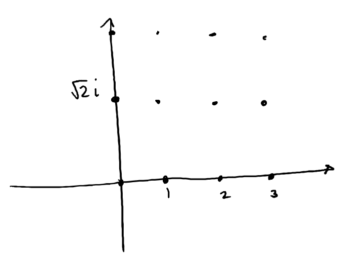
$\cup$

$$\mathcal{O}(\sqrt{D}) = \begin{cases} \mathbb{Z}[\sqrt{D}] & \text{otherwise } (D \equiv 2 \text{ or } 3 \pmod 4). \\ \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] & D \equiv 1 \pmod 4. \end{cases}$$

D negative

eg $D = -2$

$$\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} : a, b \in \mathbb{Z}\}$$



$$N(a + b\sqrt{-2}) = |a + b\sqrt{2}\,i|^2 = a^2 + 2b^2 \geq 0$$

$N(a+b\sqrt{2}) = 0 \iff a = b = 0.$

$\mathbb{Z}[\sqrt{-2}] \xrightarrow{N} \mathbb{Z}_{\geq 0}$ makes $\mathbb{Z}[\sqrt{-2}]$ a euclidean domain.

$\alpha, \beta \in \mathbb{Z}[\sqrt{-2}]$, $\beta \neq 0$.

$$\frac{\alpha}{\beta} = P_1 + P_2\sqrt{-2} \quad \text{for } P_1, P_2 \in \mathbb{Q}.$$

Up to changing $P_1 \rightsquigarrow P_1 + m$, $P_2 \rightsquigarrow P_2 + n$, $m, n \in \mathbb{Z}$

we can ensure $-\frac{1}{2} \leq P_1, P_2 \leq \frac{1}{2}$

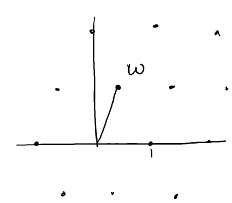
$\exists\, \gamma \in \mathbb{Z}[\sqrt{-2}]$ s.t. $\frac{\alpha}{\beta} - \gamma = P_1' + P_2'\sqrt{-2}$, $-\frac{1}{2} \leq P_1, P_2 \leq \frac{1}{2}$

$$\left|\frac{\alpha}{\beta} - \gamma\right|^2 \leq \frac{1}{4} + \frac{2}{4} = \frac{3}{4} < 1$$

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

eg $D = -3$

$\mathcal{O}(\sqrt{-3}) = \mathbb{Z}[\underbrace{\tfrac{1+\sqrt{-3}}{2}}_{\omega}]$



the above argument fails for $\mathbb{Z}[\sqrt{-3}]$

$N : \mathbb{Z}[\omega] \longrightarrow \mathbb{Z}_{\geq 0}$ $\quad N(z) = |z|^2.$

$$\frac{\alpha}{\beta} = P_1 + P_2\sqrt{-3}$$

Shift by $\underbrace{a + b\omega}_{a + b\left(\frac{1}{2} + \frac{\sqrt{-3}}{2}\right)}$ not $a + b\sqrt{-3}$

So $P_1 \rightsquigarrow P_1 + a + \frac{b}{2}$

$P_2 \rightsquigarrow P_2 + \frac{b}{2}$ for some $a, b \in \mathbb{Z}$

We can assume $-\frac{1}{4} \le P_2' \le \frac{1}{4}$

$-\frac{1}{2} \le P_1' \le \frac{1}{2}$

So $\exists\, \gamma \in \mathbb{Z}[\omega]$ s.t. $\frac{\alpha}{\beta} - \gamma = P_1' + P_2'\sqrt{-3}$

So $\left|\frac{\alpha}{\beta} - \gamma\right|^2 = \frac{1}{4} + \frac{1}{16} \cdot 3 = \frac{7}{16} < 1$ ✓

Ex: Same arg as -3 works for -7 $(-7 \equiv 1 \mod 4)$

↳ and -11

$\mathbb{Z}[\sqrt{-5}]$ is not even a P.I.D. (hence is not euclidean).

$I \subsetneq \mathbb{Z}[\sqrt{-5}]$

$\|$

$(3, 2+\sqrt{-5})$ claim: I is <u>not</u> principal.

$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$

$N(a + b\sqrt{-5}) = a^2 + 5b^2$

$N(\alpha) \ge 5$ if $\operatorname{Im}(\alpha) \ne 0$.

Let's assume $(3, 2+\sqrt{-5}) = (\alpha)$

then $\alpha\beta = 3$ for some $\beta \in \mathbb{Z}[\sqrt{-5}]$

$$|\alpha|^2 \cdot |\beta|^2 = 9$$

$|\alpha|^2 = 1 \Rightarrow \alpha = \pm 1 \Rightarrow (3, 2+\sqrt{-5}) = \mathbb{Z}[\sqrt{-5}]$ ↯

$|\alpha|^2 \neq 3$

$|\alpha|^2 = 9 \Rightarrow \beta = \pm 1 \Rightarrow \alpha = \pm 3 \Rightarrow 2+\sqrt{-5} = \pm 3\,(x+y\sqrt{-5})$ ↯

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

but primary decomposition still holds — and can be improved for such rings. (Dedekind).

Dedekind domain = Noetherian, Integral domain, & every nonzero prime ideal is maximal.

<u>Ex</u>: $D = -19$, $\mathcal{O}(\sqrt{-19})$ is a P.I.D. but not euclidean.

to prove a ring is not euclidean:

R: euclidean domain, R <u>not</u> a field.

$\exists\, u \in R$; $u \neq 0$, $u \notin R^\times$

chosen s.t. $N(u)$ is minimal wrt these conditions.
↳ in $R \setminus \{0, R^\times\}$

$\hookrightarrow$ in $R \setminus \{0, R^\times\}$

$\boxed{\text{then } \forall x \in R,\ \exists z \text{ (either 0 or a unit) s.t. } x = qu + z}$ $\longrightarrow$ Doesn't depend on particular choice of N

<u>Claim</u>: $R = \mathbb{Z}[\omega]$ with $\omega = \frac{1+\sqrt{-19}}{2}$ has no such element.

$$R = \mathbb{Z}[\omega] \xrightarrow{|\cdot|^2} \mathbb{Z}_{\geq 0}$$

$$a + b\omega \longmapsto (a + \tfrac{b}{2})^2 + \frac{19b^2}{4} = a^2 + ab + 5b^2 = |a+b\omega|^2$$

$$(a + \tfrac{b}{2})^2 + \frac{19b^2}{4} \geq \frac{19}{4} \text{ if } b \neq 0$$

assume $u \in R$ were such an element (i.e. assume R is a euclidean domain).

take $x = 2$. $R^\times = \{\pm 1\}$

$u \in R$ divides $2+0$ or $2+1$ or $\underbrace{2-1}_{\text{can't happen, } u \text{ is not a unit}}$ Since $z = 0, +1, -1$ in above notation.

$u \mid 2 \Rightarrow |u|^2 = 4$ so $b = 0$ so $u = \pm 2$ $\longrightarrow$

$u \mid 3 \Rightarrow |u|^2 = 9$ so .... so $u = \pm 3$ $\longrightarrow$ both lead to contradiction.